

Technical Reference Guide

Picis Perioperative and Critical Care 10.0C

© **Picis Clinical Solutions, Inc.** All Rights Reserved. **Picis** and the **Picis** logo may be trademarks or registered trademarks of **Picis Clinical Solutions, Inc.**, and/or its affiliates in the United States and/or other countries.

Picis Clinical Solutions believes the information in this document to be accurate and much care has been taken in its preparation. However, Picis Clinical Solutions does not accept any responsibility for the use or reliance on the information contained herein. The user should exercise care to assure that the use of the product and its related documentation is in full compliance with the laws, rules and regulations of the jurisdictions in which they are used.

Trade Secrets and Proprietary Notice: This material contains valuable confidential information of Picis Clinical Solutions and/or its affiliates and shall at all times remain the property of Picis Clinical Solutions. This material may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without the prior written approval of Picis Clinical Solutions.

Picis Clinical Solutions reserves the right to make changes to any product described in this document to modify its functionality or design. Picis Clinical Solutions is committed to duly notify its customers of any changes to product functionality or design which may affect the product performance or application. The information contained herein is subject to change and revisions may be issued from time to time. For current information, please contact Picis Clinical Solutions.

Intended Use: Picis Clinical Solutions software patient information system compiles an electronic medical record utilizing commonly available hardware, and is classified as a "medical device" by regulatory agencies in certain jurisdictions. A patient record is populated with information from various sources, such as healthcare professionals, medical devices connected to the system, and data that arrives via hospital and laboratory information systems. The application stores this information in a database, and it may analyze and/or display the data in different formats for evaluation by healthcare professionals for informational purposes. The product is intended for use by healthcare professionals.

HIPAA Compliance: Picis Clinical Solutions has put considerable effort into providing the capability to protect and audit access to patient personal health information in its products. It is highly recommended that those responsible for implementing the software fully utilize the delivered security functionality in order to ensure that only authorized users have access to the data. Picis Clinical Solutions supports configuration that will permit authorized users to restrict access to certain features and functions, to allow view-only rights to protected information and to define editing rights. Also, native audit features and reports can be utilized periodically in order to monitor changes or particular instances of access to data.

Caution: The data displayed on Picis Clinical Solutions applications are for informational purposes only. Picis Clinical Solutions recommends that users always refer to primary devices for diagnosis and treatment.

Hardware Requirements: Detailed hardware requirements are provided during the contract process. Please contact your System Administrator or Picis representative should you require additional information.

Nomenclature: The expressions "real-time data", "real-time variables", "real-time fluids" etc. are Picis expressions that refer to near real-time data collected from connected devices.



Picis Clinical Solutions, Inc.

100 Quannapowitt Parkway, Suite 405, Wakefield, MA 01880 USA

Phone: 781-557-3000 • Clientcenter@picis.com • <http://www.picis.com/>

Unique Device Identifier (UDI)	For UDI information, refer to the <i>Release Notes</i> .
--------------------------------	--

Contents

Introduction	7	Autoprint	38
About this Guide	7	Autoprint Workflow	38
Terms and Concepts	8	Autoprint Configuration	39
Technical Overview	11	Autoprint Support	40
Standard Server Configuration	11	Autoprint Maintenance	41
Standard “TPA” System	13	Troubleshoot Autoprint	41
Standalone “Clinical module” System	14	CareTaker	43
Standalone “Administrative module” System	15	Configure Caretaker for Meditech Extracts at Machine with Autoprint and Surgsync	46
Standard Server Components	16	Reporting with Crystal Reports	49
Standard System Databases	16	Connecting to Crystal Reports	49
System Backup and Recovery	17	Selecting Tables for a Report	51
Background Servers	19	Activity Logs & Diagnostic Tools	53
Overview	19	Log and Diagnostic Tools Overview	53
Server Architecture	21	SqlSpy Logs	54
Picis (web) Services	24	SQL Log Traces	55
ADT Service	24	Perfect Trace	56
Configuration Service	25	Getting Started	56
ClinicalPatientData Service	25	Display Settings	58
Demographics Service	25	Perfect Trace Messages	58
Orders Service	25	View Perfect Trace Files	59
Patient Information Service	26	Automatic Perfect Trace Files	60
Preop Service	26	Perfect Trace Log File Maintenance	61
Security Service	26	Perfect Trace Configuration	62
Web Applications	26	HL7 Outbound Messaging Log	63
PCM Service	26	ADT Administrator	63
PCM.NET Service Maintenance	27	CNLSpy	63
PCM.NET Service Troubleshooting	28	HL7InterfaceTest	63
Further Information	30	NKTSpy	63
PMR Service	30	PcmExportTestClient	64
PMR Maintenance	31	PCMTTestClient	64
Printout Service	32	Messaging Spy	64
Picis Report Service	32	Picis (web) Services Diagnostics	64
Surgsync	32	Picis (web) Services Logging Capabilities	64
Surgsync Flags	34	Picis (web) Services Diagnostics Logging Capabilities	70
CareTaker and Surgsync	37		

Contents

HL7 Outbound Messaging Log ...73

Messaging Log Overview	73
Messaging Log Configurations	73
Load Interface Outbound Message Log	
Data	75
Review Outbound Message Log Results	77
Filter Outbound Message Log Results	78
Resend Failed Outbound Messages	79
Troubleshooting the HL7 Outbound Mes-	
saging Log	81
Supported Message Errors	82

Device Connectivity85

Device Connectivity Overview	85
Medical Device Implementations	87
Recommendations	87
Potential Hardware Issues	88
Practical Examples	88
Device Drivers	92
Device Driver Contents	93
Interpreting Device Driver Diagnostic Tools	94
Troubleshooting Device Drivers	94
Perfect Trace and NKT Drivers	96
Device Data Stored in the Database	96

Additional Environments99

Create Additional Environments	99
--------------------------------------	----

Outlook Booking Appointment Settings107

Workflow Overview	107
Additional Rules for Sending Appoint-	
ments	109
Rules for Bookings	109
Rules for Surgeons and Assistants	109
Rules for Anesthesiologists	110
Calendar Feature Setup	110

Prerequisites	111
OR Manager Setup	111
Booking Outlook Email Settings	111
Autoprint Setup	112
Outlook Setup	112
Outlook SR-1 Background	113

Database Backups115

Backup Strategy	115
SQL Server Hardware	115
SQL Server Database Backups	116
Setup Backup Jobs	116
Servers/Transaction Processors	117
Spare Hardware	117

Maintenance Jobs119

Maintenance Jobs Overview	119
SQL Server Maintenance	119
Interpret the SQL Server Error Log	120
Interpret the Application Log	120
Stop and Restart SQL Server Services ...	120
Stop (or Restart) Background Servers	121
Important Notes	121
Provided SQL Server Agent Jobs	123
PSM database	123
ORM database	123
IDB database	124
TRK database	124
Missing or Additional Jobs	125
Customer Required SQL Server Agent	
Jobs	126
Downloading Files From the Picis FTP	
Site	126
Maintenance Schedule	127
Several Times per Shift	128
Hourly	128
Once a Day	128

Once a Week	129
Once a Month	129
SQL Server Password Con- figuration	131
Change the SQL Login password	131
Troubleshooting	133
Reportuser SQL Trace	135
SQL Trace Overview	135
Trace SQL User Activity	136
Required Trace Components	137
Picis Configuration Wizard	139
Picis Configuration Wizard Overview	139
Crypto Tool	143
File Integrity/Encryption/Decryption Tool Overview	143
Access the Crypto Tool	144
Hash, Encrypt, or Decrypt a File	144
Meditech Extracts	147
Meditech Extracts Overview	147
Meditech Modules	147
Magic and VMagic Extracts	147
Extract Status Message Boxes	148
TallMan Medication Update Overview	151
Running the TallMan Medication Update ..	151
Technical Notes	153
Technical Notes Overview	153
File Save Restriction	153
External Report Scheduler	154

Contents

The goal is to design an online intervention to improve the self-efficacy of service providers in a free, confidential, and secure web-based platform. The intervention will be designed to improve the self-efficacy of service providers in a free, confidential, and secure web-based platform. The goal is to design an online intervention to improve the self-efficacy of service providers in a free, confidential, and secure web-based platform.

Terms and Concepts

Term	Definition
Administrative module system	A dedicated system of services and applications running on Storage. It may also include Off Storage that services other SnapTracs. Some applications will also use Security Storage. The role used to control user and group access is included. The main administrative module system uses three databases: PDB, CDB and UDB. A SnapTrac is installed that all other systems in a cluster PDB.
API	Open Storage Service
Administrative data store	Off Storage that services other SnapTracs. The Open and the Administrative modules.
CDB	Cluster database database
Cluster module system	A dedicated system of services and applications running on a node of the following modules: Open Storage, Security Storage, PDB Storage, Cluster Local Storage. The system uses the CDB and PDB databases.
Cluster service	Module services using the cluster modules: PDB, PDB Service, Service.
Cluster status	Cluster is a representation of all of the administrative modules that are running on all nodes of the cluster. It contains the state of the cluster. The Cluster status is also used for the administrative database of the cluster global module and administrative modules. The cluster is installed using the Cluster status module.
Open CDB	The cluster and the Open administrative module databases will have shared access. This is a single database in Open and is shared by the databases in the Open and the cluster.
UDB	Cluster database
UDB	Cluster database

Suppression	Definition
Blank code	After creating a VSO2 database for the first time, the database provider is used to replicate the database for use in a VSO2 environment. The provider is not allowed to suppress the set being suppressed.
DB	DB Storage database
DBS	Security Storage database
DBS	For Replication
Page table	The user "Page table" table is the master table master table, the Replication and initial table without replication master. The user table is the table table table, for the master table the master table table is defined as the Page table through the database.
Page table and Page table	A table is a VSO2 and VSO2 environment, also the set of the VSO2 and the master and user to create additional tables in the VSO2 and the user table is a VSO2 environment. The VSO2 environment is used to building the integrated VSO2 table with using the VSO2 environment for the tablebuilding and using the VSO2 environment to create tables that can be created using the VSO2 and to replicate the VSO2 table. The VSO2 environment is also supported with the VSO2 table and VSO2. The VSO2 environment database for the VSO2 environment and the VSO2 environment is created.
Page Replication Replication VSO2 table The table is Replication Replication	Replication table is a table master table and an administrative master table with the user table table is master table table. Also other integrated tables. Master table table is the master table table and integrated table is administrative table.
Replication table	Administrative master components that can be used to create table in the VSO2 and VSO2 as administrative table (Page table, Page table, VSO2 table).
DBS	Master table database

Technical Overview

Standard Server Configuration

Flow Management and Control Suite is a distributed system that uses multiple databases stored on one server and a number of background services depending on your system.

A standard Flow server configuration is made up of a server where the application database and event, a separate server where virtual machine components are stored (usually referred to as the virtual machine server), and another server where the administrative interface components are stored (usually referred to as the administrative interface server).

Below is an example of a standard Flow server configuration. Most steps will follow the same configuration, and it varies if the needed components vary.

Note: For the rest of this guide, "virtual machine" systems can be integrated with a third-party virtual system. In this arrangement, SmartFlow is accessible from HyperVware Manager and the system can be added to the Snapshotting system. VM Manager is not used for configuration and control. The example below has not yet been used. It will change with it. The system components and configuration are identical to the suite as for a VM installation. For the system, after everything is installed, such a system should follow the VM instructions found within this guide.

For the rest of this guide, "virtual machine" systems can also be integrated with SmartFlow but in this case VM Manager is not used at all. The system components and configuration are the same as for a "standard" virtual machine installation with the addition of the VM database and VM specific settings.

Note: This Performance Protection is an optional feature and requires additional services to be purchased separately. The installation of these features is described in their respective installation guide.

Standardized "Clinical module" System

System	System Components
Database Server	Two database Two database Oracle 11g
Application server	Business Space, Intelligence, Microservices, Performance Hardware
Low virtual module server	Custom Java module, Java Components Manager, Analytics Custom Java, Customized Java code, Services, Other, Clinical Java Server
High virtual module server	Custom Java module, Java Components Manager, Analytics Custom Java, Customized Java code, Services, Other, Clinical Java Server
Low Testing PC	Intelligence Manager ¹ , 16 vCPU, 16 GB RAM, Customized Windows machine specification is kept at a minimum
High Testing PC	Intelligence Manager ¹ , 16 vCPU, 16 GB RAM, Customized Windows machine specification is kept at a minimum

1. Intel Manager is either Java Manager or Java Manager or Intel Manager.

Standard "Administrative module" System

Module	System Components
Customer Service	Live chatbot Fax chatbot Phone chat
Analytics module	Business Report, AI/Intelligence Insights, Performance Dashboard
Live administrative module (agent)	Support Center (chat, email, mobile, livechat, AI chat, Webchat, Forms, File Manager, Tools, Analytics, Contact Form, Support, AI Manager/Insight Tool, Tools, File and Settings)
Fax administrative module (agent)	Support Center (chat, email, mobile, livechat, AI chat, Webchat, Forms, File Manager, Tools, Analytics, Contact Form, Support, AI Manager/Insight Tool, Tools, File and Settings)
Live & Fax Chatting (AI)	AI Manager, Livechat, Security Manager, AI/Intelligence insights, configuration & tool of a configuration

Notes

- Your agent configuration depends on the module you are installing. For example, if you are installing AI Manager and AI/Intelligence Manager in an integrated system, you are able to have a configuration module in the system. The agent configuration also depends on the module you are installing. For example, if you are installing AI Manager and AI/Intelligence Manager, you will have a system configuration that is designed for the use of a system.
- AI Manager should have the minimum hardware specifications outlined in your agent system. For more information, please contact your AI/Intelligence.
- The information regarding the agent system is associated with Windows 7 operating systems. [See Technical Overview \(page 12\)](#).

Standard Server Components

Below is a description of the management server components:

- **Database Server:** A relational server is provided for the application databases. When MSOL and MMS databases environments are installed, a single-table server "Table" is also installed along with the installation files for all software are added.
- **File Storage Module (FMS):** The server manages integration with other storage systems such as the Storage Information System or Storage Management System for MMS Storage. (For more information, see FMS Services on page 25)
- **Backup:** The user can create backup copies to protect critical data and their external systems and transfer the data to the MMS Storage modules. (For more information, see Backup on page 25)
- **Recovery:** The user can restore software images to recovering data to MMS Storage to specified locations as specified in detail. (For more information, see Recovery on page 25)
- **File Cache Service:** The setting of operational, read and write services that supply capabilities and data to applications and other File Management and Virtual File components. (For more information, see File Cache Services on page 25)
- **Product Service:** The server controls software when using the hardware storage.
- **File Connectivity Manager (FCM):** The server manages integration with other storage systems such as the relational information system or tape drive system. It is also responsible for the introduction of information between Management and Virtual File modules. (For more information, see FCM Services on page 25)
- **System:** Customers can use to control system and configuration settings. For more information, see the System Configuration Guide.
- **Application Test Workstation:** A version of the application software will be installed to allow off-line testing and troubleshooting.

Standard System Databases

A File Management and Virtual File system requires a relational database server. The system software database is required for corresponding modules. Each module requires a different database as described in the following table.

Information Store	System Component	Function
all Storage	MSB	Manages, backing and user access information for a system
Security Storage	MSB	Manages user access rights and group security information
all	MSB	Manages, depending on all information used in a user interface system
WorkFront	MSB	Manages and reads all information related to system status for display on the WorkFront console
Power Storage Workfront Storage Power Storage Control Unit Storage	MSB	Manages all information related to system operation in the control module

Note: The actual names of your database may slightly differ, non-productive databases are prefixed by the environment name. For example: TestMSBStorage or TestMSBStorage.

System Backup and Recovery

You can work with the customer to create an environment backup and recovery strategy. In creating the strategy, consider the following points:

- **Database Server:** The database server should be regularly backed up. The user information about database connections (located in `user.ini`) file "User" table should also be backed up as it is the master source of Management and Critical User software for the site and where any user configuration files are stored.
- **Loggers:** The logs is stored on the logger management server as it is not necessary to backup anything when it needs.
- **Relayhost:** The logs is stored on the relayhost management server as it is not necessary to backup anything when it needs.
- **MSB modules files:** MSB modules include configuration and operation files that should be secured as regularly as possible settings. These files exist in the modules installation folder normally in `C:\Program Files\MSB\MSB modules folder\Settings` and in other MSB-MSB modules folder (Parameters).

- **Storage Settings:** If the user has previously selected a storage location, the message will be shown. Configuration information is stored in the USB database, and the settings are configured as follows:

3

Background Servers

Overview

This chapter describes the features and configuration of the following background server components:

Note: Not all of these components exist in all systems.

Services

- [File, Audit Services in step 10](#)
- [FTP Service in step 10](#)
- [HTTP Service in step 10](#)
- [IMAP Service in step 10](#)
- [Mail Report Service in step 10](#)

Background Applications

- [Backup in step 10](#)
- [Database in step 10](#)
- [Data Store in step 10](#)

File, web services are installed using a dedicated module. The other services and applications are installed using the Server module. The following combination determines the actual components installed. For more information, see the [File server information document](#).

The following diagram shows a typical JVM-based system.

Server Architecture

This section includes the following diagrams:

- Typical Web server architecture
- Typical Web server app flow

Note: For a traditional "internal network" system, these services, the Management dashboard, and the Content library, modules are installed on the "internal network" server.





Phone (web) Services

Phone (web) Services are the first components required to be installed on Phone (Management and Control) tools. The installer deploys the web services and web applications required for the other components and starting applications. It adds or updates database connectivity and other configuration settings. Each service has a web console for other configuration settings on screen.

The Phone (web) Services are installed on one management server, which is determined depending on the system (RTE or non-RTE). Some installed web Phone Services has a virtual database, in RTE and non-RTE, the other applications use a RT database in the same. The Phone (web) Services are configured in RTE to automatically start an agent or agent to provide better performance to the calling applications. Clients of the Phone (web) Services applications use Windows Communication Foundation (WCF) protocol to communicate with the services other than the agents. The configuration is described as part of the installation steps and the Service Installation Guide for your information.

Each service includes logging capabilities to trace errors and other messages. For information on logging, see Phone (web) Services Configuration at page 10.

Note: For more information on system server configurations, see System Server Configuration at page 11.

Note: For Phone (web) Services installation and troubleshooting information, see the Service Installation Guide appendix.

List of Phone services

- ACD Service
- Configuration Service
- Control/Intelligence Service
- Core/Registration Service
- Index Service
- Values Information Service
- Trace Service
- Security Service

ACD Service

The ACD Service facilitates the main ACD workflow, including the following ACD system operations:

Background Services

Flow Control Services

- The queue is updated
- Batch is updated
- The message is updated
- Transfer is updated
- Batch is updated
- Update an existing transfer
- Cancel an existing transfer
- Create a customer message
- Check if customer message should be automatically be changed

Configuration Service

The service stores all of the applications and other flow services in context to the database by providing the database connection string and the associated database credentials. All of the other flow services and web applications access the configuration service.

In addition to creating database connections, the configuration service stores the database user and name and password credentials in a credential table. The flow credentials user name and password is the same database. The configuration service also provides the ability to add and modify configuration data for "virtual master" applications, which are stored in the database.

Classification Services

The system that include "virtual master" the Classification Services service provides data to the Fraud Services for rules, thresholds, events, and the virtual master system.

Demographic Service

The service creates, retrieves, and updates customer demographic information between the applications and the fraud database.

The service also provides an interface to implement the integrated Fraud System.

Order Service

The system that include "virtual master" the Order service provides data to the Fraud Services for Fraud Orders, Order, Transactions, and Refundation Orders. The Order Service is also used to implement the following functionality:

- Fraud Order, Fraud Order component, Fraud Order detail component, Refundation component, Refundation detail component, Billing Order component

Background Services

PCW Service

- Patient Information/History Data
- Diagnostic order to the test laboratory
- Image enhancement
- Clinical Notes System

Patient Information Service

The Patient Information Service enables an external system to retrieve Patient Summary Data data to the other background storage Clinical Data Storage, PCW Storage, and CD Storage applications. The service also is able to retrieve Demographics, ClinicalObservations, Notes, and Plans to address the corresponding patient summary information. The PatientInformation Service also provides an interface to implement the Patient Data Store.

The Healthcare Management/Case Manager/PCW Storage applications use the API to send history to communicate with the Patient Information Service, and the Patient Information Service uses API and history to communicate with the new Clinical Patient Data, Notes, and Plans Service.

Plan Service

The system that records "clinical history" the Plan Service provides data to the Patient Summary, to images, diagnosis, and procedures.

Security Service

The service provides a single point of entry to authorization, authentication, password change, recovery, and user profiling functionality to Adaptive Clinical Data, Notes, and the Clinical History applications and other components.

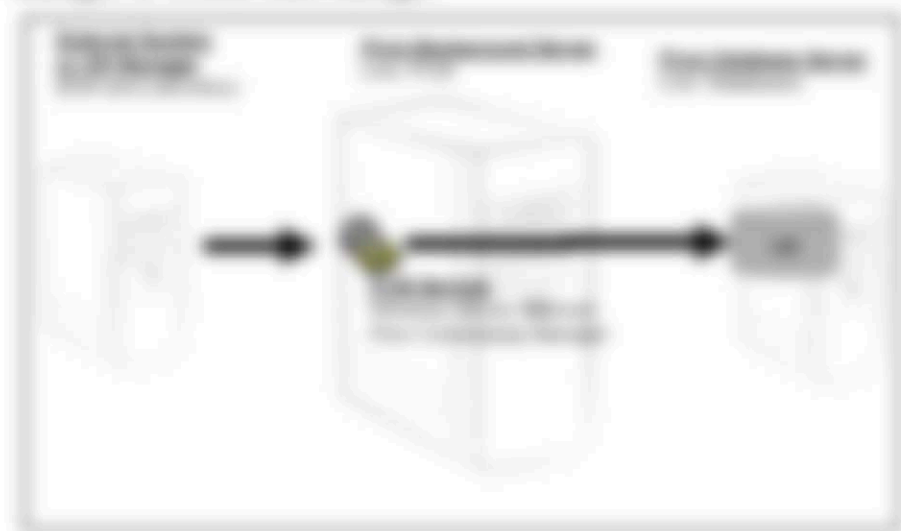
Web Applications

In addition to the individual services that are provided, the PCW web services module includes the web application that enables access to the full, high-powered configuration capabilities.

PCW Service

Flow Connectivity Manager (FCM/PCW) is a Windows service that acts as a background agent and processes messages received from external systems. FCM/PCW Service also processes the

Architectural flow of information between Mail Storage and Proxy Storage, Attachment Storage, Mailbox Storage, or Virtual User Storage



Mailbox Mail Service Maintenance

The Mailbox Mail Service maintenance consists of ensuring the Mailbox Mail Service and Mailbox Mail Service clients are working and that there is an available connection to the external systems.

A message logging tool is available to log different message activities as they are sent to Mailbox Mail. This tool must be enabled first. For more information on the Mailbox Mail message logging tool, see the Service user's manual, Tools on page 33.

Managing the Mailbox Mail Service

During system maintenance or as part of troubleshooting, you may be required to start, stop, restart or view a Mailbox Mail service.

1. Click **Start** > **Administrative Tools** > **Services** to open the Services console.
2. Right-click **Proxy Mailbox Mail Service** and select one of the following options:
 - **Stop** To stop the service. For this option to be available the service must be started.
 - **Start** To start the service. For this option to be available the service must be stopped.
 - **Restart** To restart the service.
3. Click **OK** to close the Properties window.

Configuring the Mailbox Mail Service startup type

Services should be set to start automatically. During system maintenance or as part of troubleshooting, you may be required to configure the startup type to **Manual** or **Disabled**.

Background Services

Android Services

1. Click **Step 1 – Introduction** **Tools – Services** to open the Services console.
2. Right-click **Play** **Android** **Service** and select **Properties**.
3. From the **Deployment** tab, set the **Startup type** value **Automatic**. **Manual** is disabled.
4. Click **OK** to close the Properties window.

Android Service Troubleshooting

Troubleshooting Android Service involves identifying the problem type and then working through the procedure outlined. Below is a summary of items described in this section.

- [System not seen in application console](#)
- [Missing data elements table](#)
- [Checking the Android Service messages table in the Service app](#)
- [Troubleshooting Android messages in the Service app](#)
- [Checking the Android Reported table in the Service app](#)
- [Reporting an Android Service problem in Tech Support on page 28](#)

System not seen in application console

Systems from external systems (SaaS, IoT, etc.) are not seen in **Realtime Storage**, **History Storage**, or **Virtual Case Storage**.

1. Check the **Play** **Android** **Service**. See [Checking the Android Service on the previous page](#) for further information.
2. Check the **Intermediate** table messages and all messages to **Android** **Service** and **Android** **Service** data messages. See [Checking the Android Service messages table in the Service app](#).
3. Use **Techlog** **Tools** to verify that messages are being received and if not identify what is happening. See **Techlog** **Tools** on page 25 for further details.
4. If the **Android** **Service** appears unresponsive, the primary method of message flow. See [Troubleshooting Android messages in the Service app](#) for further information.
5. Contact **Play Support**. See [Reporting an Android Service problem in Tech Support on page 28](#) for further information.

Missing data elements

A data element or value is not being reported into the SaaS database. Other elements and values in the message are being reported successfully.

1. Check the **Android Reported** table. See [Checking the Android Reported table in the Service app](#) for further details.
2. Use **Techlog** **Tools** to verify that messages are being received and if not identify what is happening. See **Techlog** **Tools** on page 25 for further details.

1. Contact [PolarSSL Support](#). Also, downloading PKCS#11 Service updates is [PolarSSL Support](#) on the web, [page 16](#) for further information.

Creating the PKCS#11 Service message table

Note: Messages sent to PKCS#11 applications must all use basic messages. Furthermore, messages sent to applications from the PKCS#11 message table in the PKCS#11 configuration file. See PKCS#11 documentation from the PolarSSL Community at [PolarSSL.com](#) for further information.

Note: The procedure is for the PKCS#11 table. If you are using another table, messages in the application table must be sent and stored, but the messages are moved from the "messages" table to the "all messages" table.

1. Messages in the table: `1. #PolarSSLApplicationMessages` (messages). If there are any messages in the table it will be because PKCS#11 cannot process them.
Processed messages are moved to: `1. #PolarSSLApplicationMessages` (messages).

Processing with PKCS#11 messages

The procedure shows how to send packets of messages to the PKCS#11. The procedure could also be applied to any PKCS#11 client.

1. Stop the PKCS#11 Service. Also, downloading the PKCS#11 Service on [page 17](#) for further information.
2. In the `1. #PolarSSLApplicationMessages` table, create the table "messages" in "messages".
3. In the `1. #PolarSSLApplicationMessages` table, create a new table called "messages".
4. Copy messages from the "messages" table to the "messages" table.
5. Stop the PKCS#11 Service. Also, downloading the PKCS#11 Service on [page 17](#) for further information.
6. Verify that the messages have processed.

Note: The application is not the only table messages at a time. In the first instance only copy of the messages in the "messages" table is only.

Creating the PKCS#11 Support table

The PKCS#11 Support table holds copies of all messages reported by the PKCS#11 and gives the reason for the reports.

1. Click **Start** -> **Programs** -> **Microsoft SQL Server** -> **SQL Server Enterprise Studio**.
2. Enter the Server name, Server name, Authentication: Login, and Password.
3. Click the **New Query** button.

Background Services

PMH Service

1. From the deployment tool, select the PMH database file and save the file. For example, it could be `pmhstorage.db`.
2. Upload the database and enable the PMH Storage service.

Reporting a PMH API Service problem to Pivotal Support

If you are experiencing problems with PMH API Service and need to open a Service Request with Pivotal Support, please include the following information:

- A detailed description of the problem, including any error code if applicable.
- A Pivotal Trace log from the PMH API Service for a time period when the problem occurred. (See [Pivotal Trace](#) on page 35 for further details.)
- From the Advanced Configuration Editor in Customer, export the configuration settings under PMH and send them to Pivotal support.

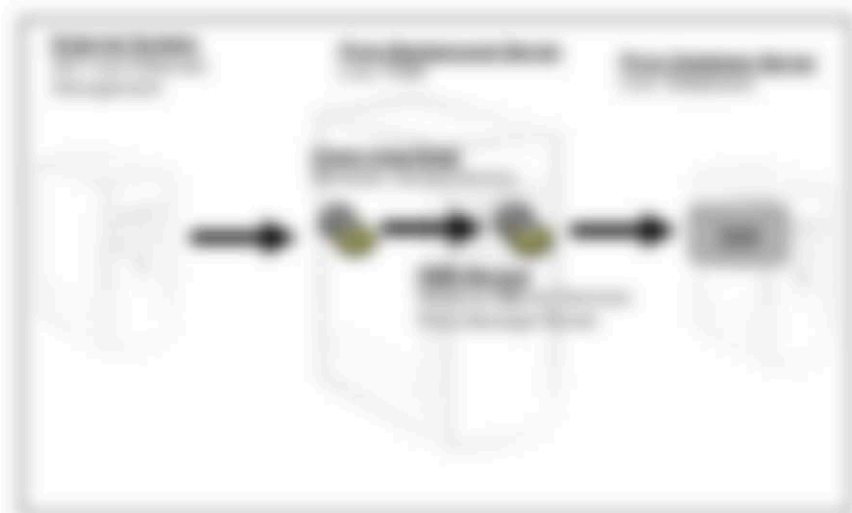
Further information

For further information about PMH API Service installation, configuration, troubleshooting and development use the PMH API Service and interface documentation from the user community at [Pivotal Tracker](#) and [Stack Overflow](#).

PMH Service

Pivotal Storage Proxy (PMH) is a Windows service that acts as the background service and processes storage requests from an external system.

The service is used by standalone "administrative control" systems and "PMH" systems.



NFS Maintenance

NFS maintenance consists of ensuring the NFS service service is running and that there is an available connection to the external system.

Starting, Stopping, Restarting, or pausing the NFS service

During normal maintenance, or as part of troubleshooting, you may be required to Start, Stop, Restart, or Pause the service.

1. Click **Start** - **Administrative Tools** - **Services** to open the Services console.
2. Right-click **File Storage Service** and select one of the following options:
 - **Start** - To start the service. For this option to be available the service must be stopped.
 - **Stop** - To stop the service. For this option to be available the service must be stopped.
 - **Restart** - To restart the service.
3. Click **OK** to close the Properties window.

Configuring the NFS service startup type

Services should be set to start automatically. During normal maintenance, or as part of troubleshooting, you may be required to configure the startup type to **Manual** or **Disabled**.

1. Click **Start** - **Administrative Tools** - **Services** to open the Services console.
2. Right-click **File Storage Service** and select **Properties**.
3. From the Startup type menu, set to **Startup type** select **Automatic**, **Manual** or **Disabled**.
4. Click **OK** to close the Properties window.

Background Services

Product Service

Product Service

The Product Service is a Spring “internal module” application. Its purpose is to generate scheduled “product” updates. A scheduled task is configured in configuration reference tables. The service behaves as follows:

1. The MicroProfile app is populated with a copy of the following events when they are downloaded to a given app:
 - `addProductInternal` `XXXXXXXXXXXX` `XXXXXXXXXXXX`
 - `addImageInternal` `XXXXXXXXXXXX` `XXXXXXXXXXXX`
 - `addImageInternal` `XXXXXXXXXXXX` `XXXXXXXXXXXX`
 - `addProductImageInternal` `XXXXXXXXXXXX` `XXXXXXXXXXXX`
 - `addProductImageInternal` `XXXXXXXXXXXX` `XXXXXXXXXXXX`
 - `addMicroProfileEvents` with an `eventType` internal `XXXXXXXXXXXX`
 - Events from the `File` `MicroProfile` app when a product update file was downloaded (internal system events, such as “Product event received”.)
2. The service gets new data in the MicroProfile app.
3. If a new event is configured to trigger a service, or if a product is scheduled for the current time, the service gets a corresponding file in the MicroProfile app.
4. The service processes the entry in the MicroProfile app and generates products according to the instructions in the MicroProfile app.

Price Report Service

For systems that include all storage, the Price Report Service (PRS) is used to generate external reports scheduled through the Report Scheduler. The external report service reports the same data at regular intervals. The data determines which scheduled reports need to be run. The service will then update a product for each of those reports which will create the report in a shared table, defined as an external destination, or not depending on configuration.

Support

Support is an application that handles and generates in the “administrative module” service. It is typically located in separate services for “DEV” and “UAT” environments.)

Support performs the following tasks:

- Update existing patient demographic data based on latest Storage Transfer (ST) information.
- Update and add Patient Management (PM) data from an external PM system.
- Process billing and PM report files.
- Merge patient medical record numbers in DB Storage.

Patient Update

When using an ST interface, Progress updates patient demographics in DB Storage by sending patient address, contact and primary to other data records as needed.

Progress checks the table update column in the ST job, and sets the job, and updates the ST update. If update is updated in other table, Progress determines if the patient address needs to be Storage. If the patient needs that the patient record in DB Storage is updated.

In transactions as that in the interface database (DB), Progress checks each transaction and determines if it is associated with a medical record number existing in an account number table. If not, the job sets that in the DB Storage database.

- If update is demographic medical record data as that in the patient's data. These are identified as all existing in the job.
- Update is information that is specific to an account number as that in the patient's account number data. These records exist in the account number as updated job. If they are not in the system, these data records are not updated because the data record in the table documentation. If not, the job sets should affect the data information from demographic data of the patient at the time of update.

DB Update

When using an ST interface, Progress adds and updates data from a DB Storage based on an ST job data table as, PM, PM, Patient record, primary.

Progress processes all data from available in DB Storage. Data from as that in DB Storage based on interface. After Progress processes data, DB determines that the data is added to the interface is not. After the processing is not, Progress processes all data from in the latest interface.

After all data from are processed, Progress checks the table update column in the ST job, and sets the job, and updates data from in DB Storage as needed.

Billing and PM Report Processing

From the main processing interface from DB Storage is used with ST and PM systems.

- Report files are automatically created when DB Storage is interfaced to Meditech PM systems.
- Standard billing and PM interface provide specifications for report files.

Tag	Description	Default Setting
<code>backgroundmode</code>	The <code>backgroundmode</code> tag specifies the type and state of the background mode. <code>backgroundmode</code> is used when <code>background</code> is specified to determine the type that will be used for the app. <code>backgroundmode</code> is used when <code>background</code> is specified to determine the type that will be used for the app.	The <code>backgroundmode</code> tag is used to specify the type of background mode that will be used for the app. The tag is used to specify the type of background mode that will be used for the app. The tag is used to specify the type of background mode that will be used for the app. <code>backgroundmode</code> is used when <code>background</code> is specified to determine the type that will be used for the app.
<code>backgroundmode</code>	The number of background mode that is used in the background mode application.	10 is the default. The tag is used to specify the number of background mode that is used in the background mode application. Note: The tag is used to specify the number of background mode that is used in the background mode application.
<code>backgroundmode</code>	Background mode only. The tag is used to specify the number of background mode that is used in the background mode application.	Background mode only. The tag is used to specify the number of background mode that is used in the background mode application.
<code>backgroundmode</code>	Background mode only. The tag is used to specify the number of background mode that is used in the background mode application.	1 is the default. The tag is used to specify the number of background mode that is used in the background mode application.
<code>backgroundmode</code>	Background mode only. The tag is used to specify the number of background mode that is used in the background mode application.	1 is the default. The tag is used to specify the number of background mode that is used in the background mode application.

Tag	Description	Minimum Setting
<code>backgroundservice</code>	The number of seconds to wait before starting the service. The service will start after the specified time has elapsed. The service will start after the specified time has elapsed.	10 seconds recommended. The minimum is 10 seconds. The maximum is 100 seconds.
<code>start</code>	1 - 10	1 - 10 seconds recommended. The minimum is 10 seconds. The maximum is 100 seconds.
<code>backgroundservice</code>	A background service that will start after the specified time has elapsed. The service will start after the specified time has elapsed. The service will start after the specified time has elapsed.	10 seconds recommended. The minimum is 10 seconds. The maximum is 100 seconds.

Configuring Autopilot activation and monitoring options in TaskPlan

1. **Open TaskPlan**
2. Click **Autopilot Properties** and choose **1. Open Autopilot Properties Properties**
3. Click **Open** and then **Autopilot Options**
4. Under **Startup Options**, click **Autopilot** and then **Minimum**
5. Under **Monitoring Options**, click **Monitor this activity**
6. Click **Yes, I'd like to Monitor** and the location of the Autopilot file in the **C:\ProgramData\Power-Data**

Autopilot

Autopilot is installed as part of the background services. Its purpose is to update changes to specified resources in a job or event. This section describes when a message is sent when a condition is satisfied. When a job is sent.

This guide covers the technical configuration of Microsoft Outlook and Office Manager. For more information, please see the following guide:

- Installing Autopilot is covered in the **Server Installation Guide**
- Enabling the functionality for specific staff members is covered in the **Security Manager User Guide**
- The rules that govern the conditions under which a message is sent are described in the **Office Manager User Guide**

Autopilot Workflow

When a condition is met, Office Manager will send a message to Outlook or another service. These changes are stored in the database. Autopilot continuously updates the database using the configured rules. When a change is made to a condition or an event, Autopilot automatically sends a job to perform verification.



For the application manual for information about configuring the system that generates the notifications.

Autoprint Configuration

All destinations, printers, and email addresses that will be used to send notifications need to be configured in the background service where Autoprint is installed.

Setting Autoprint

- In the Autoprint service, navigate to the folder "C:\ProgramData\Autoprint" and enable the Autoprint service to start Autoprint.

Configuring printers for use with Autoprint

1. In the Autoprint service, install all Windows printers that will be required as destinations.
 - In the Start Menu, click **Programs and Features** and then click **Add Features to Windows**. Follow the steps in the wizard. For more information, contact your system administrator.
2. Start Autoprint and then click **Help** to stop the opening process.
3. Click **Maintenance - Destinations** or click the Destinations maintenance button on the toolbar.
 
 The Destinations Maintenance window appears.
4. Click the **Add Printer** button.
 
 The Select Printer window appears.
5. Select the printer that is the primary to be required as destinations and then click **Next**.
6. Click **Next** and then click **Close**.

Configuring Email for use with Autoprint

1. In the Autoprint service, install Outlook.
2. Start Autoprint and then click **Help** to stop the opening process.

Background Services

Autopilot

1. Click **Windows -> Destinations** or click the **Destinations** maintenance button on the toolbar .
The **Destinations Maintenance** window appears.
2. Click the **Import Email** button.
3. Select the email addresses you want to import and then click **Import** to import email addresses to the destination list.
4. Click **Done** and then click **Close**.

Importing e-mail to email destination

This procedure shows how to import e-mails to a group or email address from the destination list.

Note: A destination cannot be deleted if it is included in an Autopilot rule.

1. Stop Autopilot and then click **Stop** to stop the scanning process.
2. Click **Windows -> Destinations** or click the **Destinations** maintenance button on the toolbar .
The **Destinations Maintenance** window appears.
3. Select a destination in the list and click **Import**.

Autopilot Support

The main support task for Autopilot is ensuring that the application executable is installed.

- Place Autopilot in the **All Users** user folder so any user who logs on will receive Autopilot.
- Use **Customize** to maintain Autopilot. After **Customize**, go to any of the main screens.

Note: Autopilot will periodically stop based on a counter, usually that can be set to any number of minutes. This is useful when there is a delay. The default is 30 minutes. After Autopilot stops, **Customize** will start it.

- The default stop/restart procedure to be followed if the screen stops responding.

Configuring Autopilot installation options in Customizer

1. Stop Customizer.
2. Click **File Properties** and change to **File Properties** (Autopilot Manager) and
3. Click **Open**.
The process is added to the Customizer window.
4. Click the **Options** button.
The **Options** window appears.
5. Under **Display Options**, select **Auto Stop** and **Auto Maintenance** and then click **OK**.

1. In the **Configuration** window, click the **Web Page** button.

Autopilot Maintenance

Autopilot should be running at all times.

- If it is processing items in the queue, the processing queue status bar displays the item that is currently being processed.
- If there are no items in the queue, the processing queue status bar displays the message **Processing**.
- If Autopilot is not running, the processing queue status bar will display the message **Not Running**. To fix, pressing the **Refresh** button.

Troubleshooting Autopilot

You should only activate these troubleshooting procedures after consultation with Pave Support.

Activating Autopilot Logging

This procedure enables a log which logs Autopilot's application activity. The log file is named *autopilot.log*, located under the application's **Support** > **Resources** > **Logging** log file.

Note: The log file should be deactivated when no troubleshooting is needed as it can cause slow application performance.

1. Click **Autopilot**.
2. In the Autopilot panel, browse to the folder "C:\ProgramData\Pave\Autopilot" and double-click the file **Autopilot** or its equivalent in a Windows.
3. Under the **Application** section, type the following command:

```
set log on
set debug on
```

4. Click and save **Autopilot** as.
5. Restart Autopilot.

Activating Autopilot Logging

1. Click **Autopilot**.
2. In the Autopilot panel, browse to the folder "C:\ProgramData\Pave\Autopilot" and double-click the file **Autopilot** or its equivalent in a Windows.
3. Under the **Application** section, enter the following command:

```
set log on
set debug on
```

Background Services

Overview

1. Create and start `Background` job
2. Remove `Background`

Note: This job can also control the persistence, such as adding a new value to `cache` and so on.

Turning the auto-persistence or database logging on

This procedure assumes that the background service has database logging activated. See [creating database logging in the database](#) page for further details.

- In the `Background` service, access to the table `CS_FragmentationHistory` is enabled for the auto-persistence or to add it to `Background`.

Activating `Background` logging about logging

This procedure enables using the `Background` job, `cache`, `Logging` or `CS` storage module to store logging in `Background` jobs.

Note: The log file should be distributed when no auto-persistence is enabled because it will cause the application to run slowly.

- In the `CS` database, set the `Background` job, `cache`, `Logging` or `CS` storage module to activate logging in `Background`.
To activate logging in `Background`, create and file a new logging in `CS` storage to add at least one job to `Background`. It will be working logging.
Start the logging and check to see if `Background` joined the job. If not, check the log file.

Deactivating `Background` logging about logging

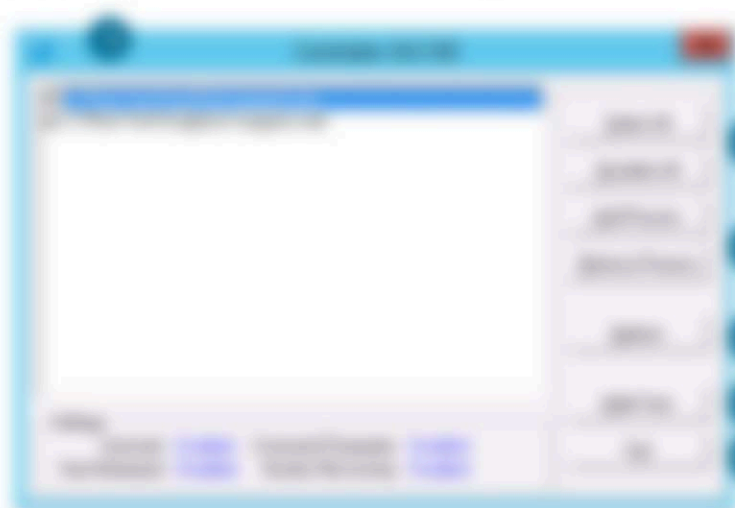
- In the `CS` database, set the `Background` job, `cache`, `Logging` or `CS` storage module to deactivate logging in `CS`.

Turning the `Background` job, `cache`, `Logging` or `CS` storage logging on

- In the `CS` storage configuration, access to the `CS` table and modules for the `Background` job, `cache`, `Logging` or to add it to `Background`.

CuraTracer

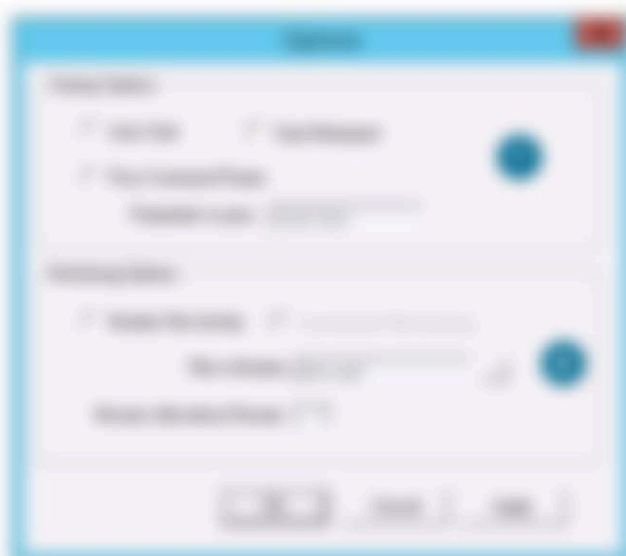
CuraTracer is used to monitor management applications. CuraTracer is always running in an active state. CuraTracer monitors CuraTracer to automatically monitor these applications when they start. CuraTracer has the following options:



1. **Monitor CuraTracer:** Monitor CuraTracer can be monitored continuously.
2. **Monitor CuraTracer:** Monitor CuraTracer can be monitored with CPU, Memory, and CPU. Monitor CuraTracer can be monitored with CPU.
3. **Monitor CuraTracer:** Monitor CuraTracer can be monitored with CPU.
4. **Options:** Monitor CuraTracer can be configured using options.
5. **Help:** Monitor CuraTracer is started for running in the background with the user. Monitor in the Help bar.
6. **Help:** Monitor CuraTracer.

Background Services

Overview



- 1. **General Options:** Configures the general options for the application.
- 2. **Monitoring Options:** Configures if all selected processes are monitored when the application starts. It is recommended this is always selected.
- 3. **Start Monitoring:** Configures if all selected processes are started monitored.
- 4. **Stop Monitoring:** Configures if all selected processes are stopped monitored.
- 5. **Monitoring Interval:** Configures the interval to be applied to the monitoring.
- 6. **Monitoring Unit:** Configures the unit to be applied to the monitoring.
- 7. **Monitor the Activity:** Configures if the activity is monitored.
- 8. **Use Memory:** Configures if the memory is monitored.
- 9. **Use CPU:** Configures if the CPU is monitored.
- 10. **Use Disk:** Configures if the disk is monitored.
- 11. **Use Network:** Configures if the network is monitored.
- 12. **Use I/O:** Configures if the I/O is monitored.
- 13. **Use System:** Configures if the system is monitored.
- 14. **Use User:** Configures if the user is monitored.
- 15. **Use Group:** Configures if the group is monitored.
- 16. **Use Process:** Configures if the process is monitored.
- 17. **Use Thread:** Configures if the thread is monitored.
- 18. **Use File:** Configures if the file is monitored.
- 19. **Use Directory:** Configures if the directory is monitored.
- 20. **Use File System:** Configures if the file system is monitored.
- 21. **Use File System:** Configures if the file system is monitored.
- 22. **Use File System:** Configures if the file system is monitored.
- 23. **Use File System:** Configures if the file system is monitored.
- 24. **Use File System:** Configures if the file system is monitored.
- 25. **Use File System:** Configures if the file system is monitored.
- 26. **Use File System:** Configures if the file system is monitored.
- 27. **Use File System:** Configures if the file system is monitored.
- 28. **Use File System:** Configures if the file system is monitored.
- 29. **Use File System:** Configures if the file system is monitored.
- 30. **Use File System:** Configures if the file system is monitored.
- 31. **Use File System:** Configures if the file system is monitored.
- 32. **Use File System:** Configures if the file system is monitored.
- 33. **Use File System:** Configures if the file system is monitored.
- 34. **Use File System:** Configures if the file system is monitored.
- 35. **Use File System:** Configures if the file system is monitored.
- 36. **Use File System:** Configures if the file system is monitored.
- 37. **Use File System:** Configures if the file system is monitored.
- 38. **Use File System:** Configures if the file system is monitored.
- 39. **Use File System:** Configures if the file system is monitored.
- 40. **Use File System:** Configures if the file system is monitored.
- 41. **Use File System:** Configures if the file system is monitored.
- 42. **Use File System:** Configures if the file system is monitored.
- 43. **Use File System:** Configures if the file system is monitored.
- 44. **Use File System:** Configures if the file system is monitored.
- 45. **Use File System:** Configures if the file system is monitored.
- 46. **Use File System:** Configures if the file system is monitored.
- 47. **Use File System:** Configures if the file system is monitored.
- 48. **Use File System:** Configures if the file system is monitored.
- 49. **Use File System:** Configures if the file system is monitored.
- 50. **Use File System:** Configures if the file system is monitored.
- 51. **Use File System:** Configures if the file system is monitored.
- 52. **Use File System:** Configures if the file system is monitored.
- 53. **Use File System:** Configures if the file system is monitored.
- 54. **Use File System:** Configures if the file system is monitored.
- 55. **Use File System:** Configures if the file system is monitored.
- 56. **Use File System:** Configures if the file system is monitored.
- 57. **Use File System:** Configures if the file system is monitored.
- 58. **Use File System:** Configures if the file system is monitored.
- 59. **Use File System:** Configures if the file system is monitored.
- 60. **Use File System:** Configures if the file system is monitored.
- 61. **Use File System:** Configures if the file system is monitored.
- 62. **Use File System:** Configures if the file system is monitored.
- 63. **Use File System:** Configures if the file system is monitored.
- 64. **Use File System:** Configures if the file system is monitored.
- 65. **Use File System:** Configures if the file system is monitored.
- 66. **Use File System:** Configures if the file system is monitored.
- 67. **Use File System:** Configures if the file system is monitored.
- 68. **Use File System:** Configures if the file system is monitored.
- 69. **Use File System:** Configures if the file system is monitored.
- 70. **Use File System:** Configures if the file system is monitored.
- 71. **Use File System:** Configures if the file system is monitored.
- 72. **Use File System:** Configures if the file system is monitored.
- 73. **Use File System:** Configures if the file system is monitored.
- 74. **Use File System:** Configures if the file system is monitored.
- 75. **Use File System:** Configures if the file system is monitored.
- 76. **Use File System:** Configures if the file system is monitored.
- 77. **Use File System:** Configures if the file system is monitored.
- 78. **Use File System:** Configures if the file system is monitored.
- 79. **Use File System:** Configures if the file system is monitored.
- 80. **Use File System:** Configures if the file system is monitored.
- 81. **Use File System:** Configures if the file system is monitored.
- 82. **Use File System:** Configures if the file system is monitored.
- 83. **Use File System:** Configures if the file system is monitored.
- 84. **Use File System:** Configures if the file system is monitored.
- 85. **Use File System:** Configures if the file system is monitored.
- 86. **Use File System:** Configures if the file system is monitored.
- 87. **Use File System:** Configures if the file system is monitored.
- 88. **Use File System:** Configures if the file system is monitored.
- 89. **Use File System:** Configures if the file system is monitored.
- 90. **Use File System:** Configures if the file system is monitored.
- 91. **Use File System:** Configures if the file system is monitored.
- 92. **Use File System:** Configures if the file system is monitored.
- 93. **Use File System:** Configures if the file system is monitored.
- 94. **Use File System:** Configures if the file system is monitored.
- 95. **Use File System:** Configures if the file system is monitored.
- 96. **Use File System:** Configures if the file system is monitored.
- 97. **Use File System:** Configures if the file system is monitored.
- 98. **Use File System:** Configures if the file system is monitored.
- 99. **Use File System:** Configures if the file system is monitored.
- 100. **Use File System:** Configures if the file system is monitored.

Note: The application and monitoring options are not used for all processes that are in the instance of the application. If necessary, multiple instances of the application can be running to allow different configurations.

The following management applications need to be monitored by the application:

Process Name	Management Application
C:\Program Files\Background Services\Background Services.exe	Background
C:\Program Files\Background Services\Background Services.exe	Background

The application needs the Windows process identifier for each process added to the process list. When the application starts a process, it records the associated process identifier that Windows assigns to the process. The value of the process identifier can then be used to identify the process. If any of the registered processes stop, and the application needs to determine whether the process identifier, the application will record the process.

Note: The application should be added to the system tray of the application. This will allow the application to start when the background service starts.

Starting Coroutine

- 1 Double-click the `Coroutine` icon in the desktop.
 - a
- 2 Browse to the folder "C:\Program Files\Coroutines" and double-click `Coroutine` icon. Assuming the `Coroutine` is installed in the default folder.

Adding Coroutine to the Task Bar

- 1 Click **Add** button in the `Coroutine` window.

Stopping Coroutine from the Task Bar

`Coroutine` is started task button in the task bar.

- 1 From the task bar, double-click the `Coroutine` icon (blue button).

Uninstalling Coroutine

- 1 Click **Quit**.
 - a
- 2 Click the **X** in the top right-hand corner.

Adding an Executable File

- 1 Start `Coroutine` then click **Add Process** and browse to the executable file to be added.
- 2 Click **Open**.
- 3 Select the file and the executable file is be added.

Stopping an Executable File

Use this procedure to stop any of the transaction processes that are selected but not started.

- 1 From the task bar, double-click the `Coroutine` icon (blue button) or start `Coroutine`.
- 2 Select the file and to the executable file is be started.

Stopping an Executable File

Use this procedure to stop any of the transaction processes.

- 1 From the task bar, double-click the `Coroutine` icon (blue button).
- 2 Click the file and to the executable file is be stopped.

Configuring startup options

- 1 Start `Coroutine` and click **Options**.
- 2 Select the file and any of the following options.

Background Services

CardFlow

- **Available** (boolean): If all selected accounts are loaded when CardFlow starts. If not, automatically this is always added.
- **Not Monitored** (boolean): If all selected accounts are loaded manually.
- **Has Unsynced Records** (boolean): Indicates the operation is to be added to the accounts.

Configuring monitoring options

1. Open CardFlow and click **Options**.
2. Select the way of the following options:
 - **Monitor the Activity** (boolean): If the will be monitored.
 - **Use Monitor the Activity** (boolean): Specifies the strategy when monitoring is used for Budgets and Expenses, while Monitor Accounts will be on the same machine.
 - **File to Monitor** (text): Type the name of the file.
 - **Monitor the entire Range** (boolean): If checked, the file will be without activity before CardFlow records the application.

Configuring CardFlow to use automatically

1. Go to the folder "C:\Programs\CardFlow\".
2. Assuming CardFlow is installed in the default folder.
3. Right-click CardFlow.exe and select **Create Shortcut**.
4. Right-click Shortcut to CardFlow.exe and select **Task**.
5. Go to the Start Menu program folder "C:\Programs\CardFlow\Task\TaskProgram\".
6. Right-click in the folder and select **Task**.

Configure CardFlow for Monitor Accounts at Machine with Autoprint and Budgets

The user, using the Monitor the Activity option in CardFlow for Budgets and Expenses, and also using CardFlow for Monitor Accounts at the same machine, requires automatic load each file each month.

After CardFlow has been installed and configured for Budgets and Expenses, follow these steps to configure CardFlow for use with Monitor Accounts. If CardFlow is used to both on the same machine.

Creating a CardFlow Shortcut to Monitor Accounts

1. Go to the folder "C:\Programs\CardFlow\" and create a copy of the "CardFlow" folder.
 2. Rename the new folder as "CardFlowAccounts\".
- This is the directory that is designated for use with Accounts.

3. In the "CertificateManager" node, double-click the the Certificate used to sign Certificate.
4. Click the **Key Properties** button and add the Certificates to this instance of Certificate.
Note you should have one instance of Certificate configured to manage Certificate and Signature, and another instance of Certificate configured to manage Certificates.

Configuring the monitoring Signature and Signature with multiple Certificate instances

1. Browse to the node "CertificateManagerCertificate" and click Certificate.
2. Click the **Options** button.
3. Under Monitoring Options, select the **Monitor File Integrity** checkbox and the the **Monitor File Ownership** checkbox.
4. In the File to Monitor field, type the name of the file to monitor.
5. Click **OK** and close or minimize the Certificate window.

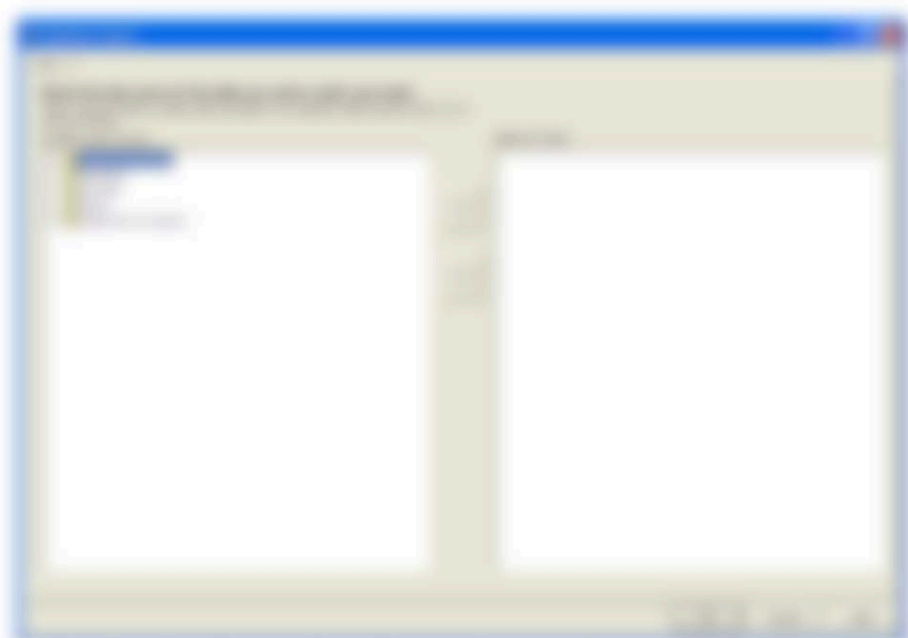
4

Reporting with Crystal Reports

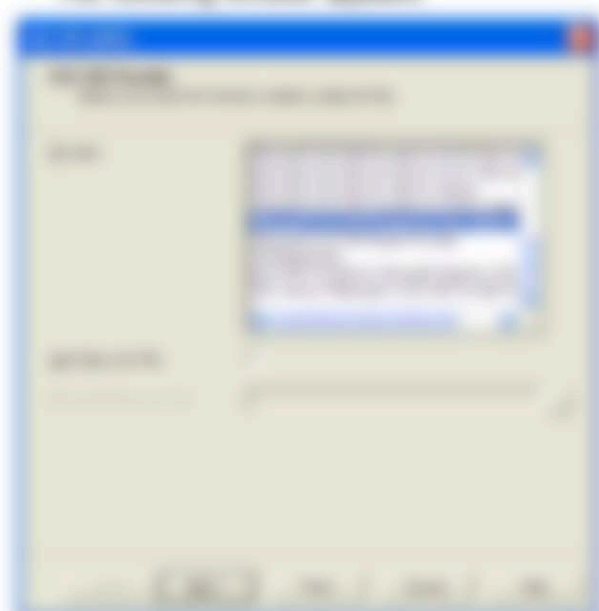
Connecting to Crystal Reports

Crystal Reports should be connected to the ODBC database via ODBC.

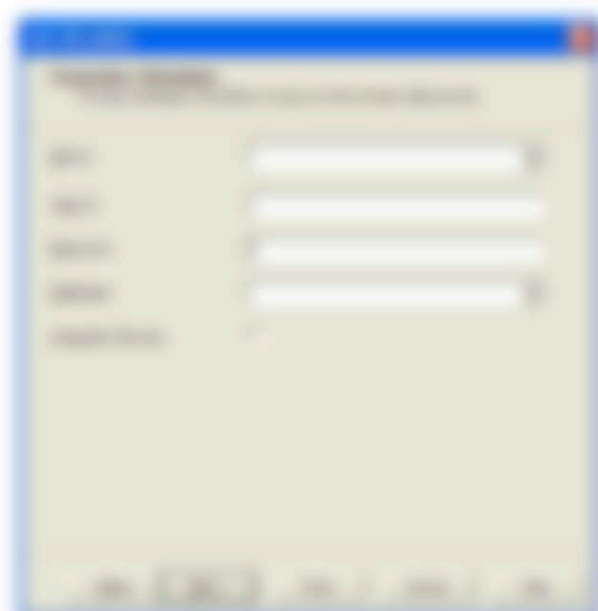
1. Open Crystal Reports
2. Open File - New
The Crystal Reports Gallery window appears.
3. Select using the Report Wizard and then New
The Database Crystal window appears.



- a. Double-click **Microsoft SQL Server** in the list of data sources.
 - b. Double-click **Microsoft SQL Server** in the list of data sources.
- The following window appears:



- c. Enter **Microsoft SQL Server** in the 'Server' field and click **OK**.
- The following window appears:



1. Specify the following details in the corresponding fields:
 - a. In **Table**, select your HR Manager schema from the drop-down box or type the IP address.
 - b. In **Table ID**, enter the user name for the database user.

Note: In previous releases, the application database user was selected. The user will connect to data and update if it was at your site. In a previous release, the application is no longer selected or supported. This is to ensure compliance with security standards. When you create online Crystal Reports, use a database user that has sufficient access to the application database.

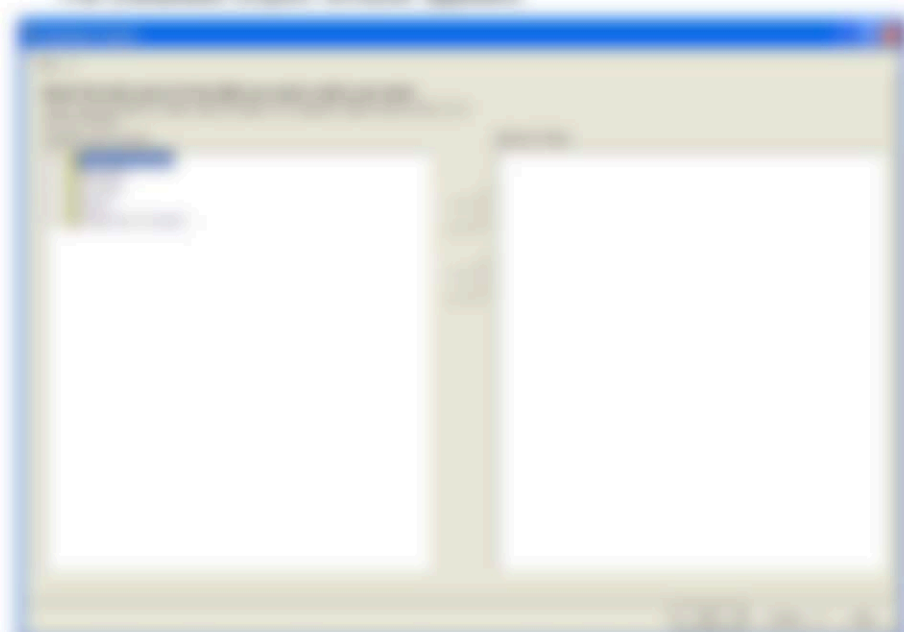
- c. In **Password**, enter the user name for the database user.
 - d. In **Database**, select your HR Manager database from the drop-down box.
2. Click **Next**.
The relevant information window appears.
3. Click **Next** to complete the wizard.

Selecting Tables for a Report

After you have connected to Crystal Reports, you can select tables and create reports.

1. Open Crystal Reports.
2. From the File menu, click **New**. The Crystal Report Wizard window appears.
3. Select **Using the Report Wizard** and click **Next** (you must also select a Data Source).

The Database Report window appears



1. Double-click **Database Connections** and navigate to the **Microsoft** and then click the **Server** name of the connection you created.
2. Highlight a table or view and click the **+** button to select the table.
3. Click **OK** to complete.

Activity Logs & Diagnostic Tools

Log and Diagnostic Tools Overview

This chapter includes and links to the tools available for logging application activity, and a variety of other diagnostic tools. Below is a list of these tools, with details on where you can find more information on the log.

The diagnostic tools are available at both workstation and server:

- **Windows Server** – [“Using Diagnostic Tools”](#)
- **Windows Desktop** – [“Program Files Collection Tools”](#)

Log files are typically stored in the following workstation folder:

- [C:\ProgramData\Microsoft\](#)

This chapter includes descriptions of the following diagnostic tools:

- [Event logs](#) on the next page
- [SQL Performance](#) on page 15
- [SQLSrv](#) on page 15
- [Flow Configuration Wizard](#) on page 15
- [SQL Server Profiler](#) on page 15
- [SQL Server Enterprise Manager](#) on page 15
- [SQLSrv](#) on page 15
- [Performance Monitor](#) on page 15

- ▶ [What's new in Surflog 1.0](#)
- ▶ [Surflog: How to use it](#)
- ▶ [Surflog: How to install it](#)

Surflog Logs

Surflog is a diagnostic tool used to log application and management service activities. Surflog logs can be used to audit the following applications and services:

- ▶ [iSCSI Manager](#)
- ▶ [SmartTrack](#)
- ▶ [Security Manager](#)
- ▶ [Triggers](#)
- ▶ [Traps](#)

Surflog can record the following types of application activity:

- ▶ **Surflog log** This records all SQL statements sent from the host machine to application's database.
- ▶ **Setting logs** This records application commands that can be interpreted by a database.

Note: Unlike Profiler Trace, there is no administrator file for Surflog — the logs are activated from within iSCSI Manager.

Logs depend on the selected trace activation. The log files will be generated with messages until the application is closed in the log file are deactivated. When the application is opened, the old log is deleted and a new log file is created.

The log files are saved in the Common Application Directory, in subdirectories and services in `C:\ProgramData\HDS\HDS\...`

The file format is as follows:

- ▶ **SQL or trace activation**
 - ▶ `msdsqlsurflogging_YYYYMMDD_XXXXXXXXXX.sql`
- ▶ **SQL or trace service**
 - ▶ `msdsqlsurflogging_YYYYMMDD_XXXXXXXXXX_YYYYMMDD_XXXXXXXXXX.sql`

Activating the Surflog log

- ▶ In iSCSI Manager, click **Tools** → **Options** → **SQL Log** file.
The tool is visible in the toolbar when logging is active.

Restarting the WebLog.log

1. In IIS Manager, click **Tools** > **Options** > **Web Log** IIS.

Restarting the WebLog.log

1. In IIS Manager, click **Tools** > **Options** > **Restarting the WebLog.log** to restart the service when logging is active.

Restarting the WebLog.log

1. In IIS Manager, click **Tools** > **Options** > **Restarting IIS**.

Web Log Traces

When WebLog traces are active, the traces are logged to files. To help with troubleshooting, you can open or export the log files and view the log files as you perform actions in the application.

Note: The first action in a log file is the first time you use the IIS Manager.

Restarting the WebLog.log

1. In IIS Manager, click **Tools** > **Options** > **Web Log** IIS.
2. Type the name of the file in the open provided and click **OK**.

Restarting the WebLog.log

1. In IIS Manager, click **Tools** > **Options** > **Restarting IIS**.
2. Type the name of the file in the open provided and click **OK**.

Restarting the WebLog.log and the WebLog.log with the application open

1. Open IIS Manager. If it is not already open.
2. Browse to the folder "C:\ProgramData\Microsoft\..." and open the file WebLog.log using a text editor such as Notepad.
3. Add the following information under the **Log File** section:

```
Log File: C:\ProgramData\Microsoft\...
Log File: C:\ProgramData\Microsoft\...
```

Note: The file is updated. It keeps the service in use.

4. Save and close the file WebLog.log.

Activity Logs & Diagnostic Tools

Performance

1. Open VM Manager and activate one of the log files. When configuring the settings, you can select VM or ESX/ESX Host. Selecting the VM log file, the information page for further information.
When you use VM Manager the traces will be visible in a window.

Performance Traces

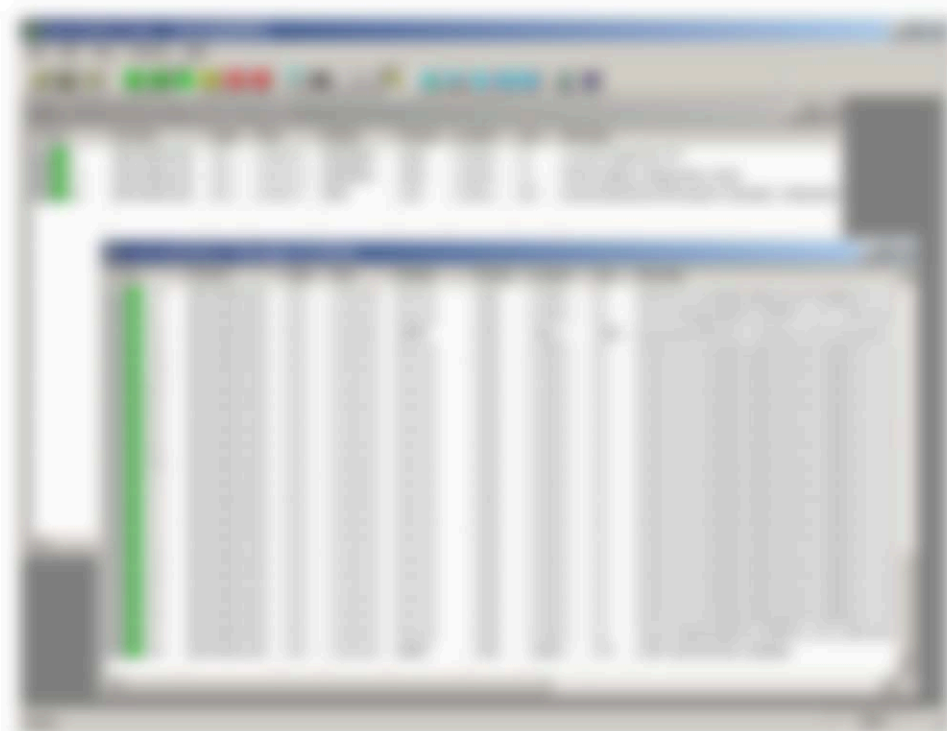
Performance Traces is a diagnostic tool used to log Performance and Virtual Tools application and management activities. Performance Traces can be used to audit the following applications and services:

- Hostname Manager, Policy Manager, or Virtual Tools Manager
- Proxy Manager
- Virtual Tools System
- The VMX service

Note: Traces will only be "Diagnostic Tools" system logs to open Performance Traces. See your Proxy system administrator if you are not able to open Performance Traces.

Getting Started

When Performance Traces is open it automatically records application activity for all compatible applications that are installed on the workstation. Performance Traces opens one window for each Performance and Virtual Tools module it monitors located on the workstation or remote. In the graphic above, two modules are open on the workstation.



Typically, Perfmon Tools is used to detect application activity when abnormal behavior is being observed. The following activities would be used:

1. Open Perfmon Tools on the WindowsServer2008
2. Start the application/service you want to monitor
3. Perform the steps required to use the abnormal behavior
4. Save the Perfmon Tools file and export it to File Support

Perfmon Tools, when running in the interactive mode, stores logging information in memory. During extended periods there is the issue of logging, using Perfmon Tools, a limitation is performance/performance might be affected. Using Perfmon Tools and logging across the system. As you work with Perfmon Tools, you should collect your own logging to with the length of time Perfmon Tools can be used without causing performance problems.

Setting Perfmon Tools

1. Open Perfmon Tools by double-clicking the file PerfmonTools.exe in one of the folders below:
Windows Server 2008: C:\ProgramData\Microsoft\Windows\PerfmonTools\PerfmonTools.exe
Windows 7: C:\ProgramData\Microsoft\Windows\PerfmonTools\PerfmonTools.exe
2. Enter a valid user name and password to log on.

Activity Log & Diagnostic Tools

Perfmon Trace

Creating Perfmon Trace

- 1. Click **File** menu > **Save**

Setting up Perfmon Trace file

1. Open Perfmon Trace
2. Select a variable
3. Click **File** > **Save**
4. In the space provided enter a file name and click **Save**
The entire variable is saved as a file with the extension .CSV

Display Settings

By default, a maximum of 10 CSV files are visible in each variable. This means if the file you are viewing contains more than 10 CSV files, not all are visible.

Changing the viewing variables

1. Open Perfmon Trace
2. Select a variable
3. Click **File** > **Maximum displayed messages**
4. In the space next to **Maximum messages** enter a numeric value
5. Click **OK** when you have finished

Perfmon Trace Messages

Perfmon Trace displays the following information for each message:



Severity	Time	Message	Source
Warning	10/10/2010 10:10:10 AM	Warning message	Source 1
Error	10/10/2010 10:10:10 AM	Error message	Source 2
Information	10/10/2010 10:10:10 AM	Information message	Source 3
Warning	10/10/2010 10:10:10 AM	Warning message	Source 4
Error	10/10/2010 10:10:10 AM	Error message	Source 5
Information	10/10/2010 10:10:10 AM	Information message	Source 6
Warning	10/10/2010 10:10:10 AM	Warning message	Source 7
Error	10/10/2010 10:10:10 AM	Error message	Source 8
Information	10/10/2010 10:10:10 AM	Information message	Source 9
Warning	10/10/2010 10:10:10 AM	Warning message	Source 10

- **Severity** Severity being observed in the message. It will be either Information, Critical, Error, Warning, or Fatal Warning
- **Time** The time the message was recorded
- **Message** Source message
- **Source** Source Name
- **Storage** Type of the message

Setting up Perfmon Trace message alert

1. In Perfmon Trace, double-click a message

The Trace Description window appears displaying details of the selected message.

1. Click  when you have finished.

View Packet Trace Files

Packet Tracer produces many messages, some of which are not always relevant to the problem you are troubleshooting. Using the filtering options, the number of visible messages can be reduced.

Opening a Packet Trace File in a window

Packet Tracer files can be opened at the same time as the application sends messages to the file.

1. Open Packet Tracer and then start an application.

The file is displayed.

Opening a Packet Trace File

1. Double-click a packet trace file (.PTB).
2. Enter a valid user name and password to log on to the system.

The file is displayed.

Filtering by severity

Each message in Packet Tracer is assigned one of the following severities: Critical, Error, Information, Warning, or Not Set.

When you select a severity, you can view any message whose severity is equal to or higher than the one you choose. For example, if you select Information, you can view Information, Error, and Critical messages.

1. Open Packet Tracer.
2. Click **View > Files**.
3. From the Severity drop-down menu, select a filtering level (eg, Not Set).
4. Click  to return to the results window.

Filtering by name, interface, source, file, and time

The Traces, Messages, Trunks, Files and Links lists contain can be set that can either be included or excluded.

1. Open Packet Tracer.
2. Click **View > Files**.
3. In the appropriate list type the search text.
4. If this is to be included select the box next to **Included**.
5. Click  to return to the results window with the filter applied.

Activity Log & Diagnostic Tools

Perfmon Trace

Planning the Trace

There are two options to trace system data. This is particularly useful when you want to trace a specific feature or subsystem in the FIM system.

1. Open Perfmon Trace.
2. Click **File** > **Trace**.
3. In the new pane to create Manager or Formula Manager type the system name.
4. Select the new pane to **Select all features** to capture the complete system.
With this option selected, you would select only those elements with the option checked that would report hardware, software, and hardware.
5. Select the new pane to **Specify data** to capture operations of code.
With this option selected, you would select only those elements with the option checked that would report logs, events, and errors.
6. Click **OK** to start in the results window with the filter applied.

Automatic Perfmon Trace Files

Perfmon Trace can run automatically without being open. When automatic mode is enabled, Perfmon Trace files are stored in the following locations:

- Windows 7: C:\ProgramData\Microsoft\
- Windows Server: C:\ProgramData\Microsoft\PerfmonTrace\

Installing automatic Perfmon Trace file collection

1. Open Perfmon Trace, if necessary.
2. Choose the location folder and open the file Properties dialog box only.
Windows 7: C:\ProgramData\Microsoft\PerfmonTrace\
3. Set trace settings as follows:

System not traced?

Do you want to trace all the features that report events?

Note: This will trace the entire system trace file, which is saved, not the entire path to the trace.

4. Click **OK** and save the file.
The system trace or application is enabled, trace files are automatically saved in the folder you've specified in one of the following locations:
Windows 7: C:\ProgramData\Microsoft\PerfmonTrace\

Changing the trace file destination

1. Open Perfmon Trace, if necessary.

2. Browse to a location where you will save the log files (for example, locally).

Windows 7: C:\Program Files\Microsoft

Windows Server: C:\Program

3. Edit the `TraceOptions` setting to specify the save folder for trace files.

Note: This value for `TraceOptions` must have the correct file format, or the entire path is the folder.

4. Close and save the file.

The save folder an application is running, trace files are automatically saved to the folder you've specified. It is one of the following locations:

Windows 7: C:\Program Files\Microsoft\TraceOptions

Windows Server: C:\Program Files\Microsoft\TraceOptions

Perform Trace Log File Maintenance

Purview Trace log files are not automatically saved. Instead, a utility called `TraceOptions` is provided to automatically purge trace files. Using `TraceOptions`, you can purge log files in all active paths by specifying a command. It also can schedule a scheduled purge to delete files that are older than a specified number of days that are configured.

With each option, you can specify the folder that which log files should be deleted. The folder specified is optional. If a folder is not specified, log files are deleted from the default logging folder which is configured with the `TraceOptions` value in the `TraceOptions` utility file. For more information, see [Automatically Purge Trace Files in the Purview Log](#).

Note: Automatic purge is required to configure `TraceOptions`.

Manually purge the logs that 30 days

1. Open Command Prompt using **Run as Administrator**.

2. Type one of the following commands, depending on your machine:

Windows 7: C:\Program Files\Microsoft\TraceOptions\tools\TraceOptions.exe /purge /days:30

Windows Server: C:\Program Files\Microsoft\TraceOptions\tools\TraceOptions.exe /purge /days:30

Where `TraceOptions` specifies the number of days that which log files will be deleted. The value for the number is `30` days.

`/purge` is the folder where the log files are stored. This is optional, include to use the default location.

3. Press **ENTER**.

Schedule an automatic log file purge

1. Open Command Prompt using **Run as Administrator**.

Activity Log & Diagnostic Tools

Perfmon Trace

1. Type one of the following commands, depending on your machine:

Windows 7, 8, 10: `tracelog -file \\localhost\perfmontrace.log -maxsize 1000000000 -maxduration 10000000000`

Windows Server 2008, 2012, 2016: `tracelog -file \\localhost\perfmontrace.log -maxsize 1000000000 -maxduration 10000000000`

Where `tracelog` is the command used to start and

`\\localhost\perfmontrace.log` specifies the location of the log file and setting up the file will be created. The size for the number of MBs and

`10000000000` is the value where the log file will store data. It is optional, because it can be added manually.

2. Press **ENTER**.

Generating a Perfmon Trace log file is a two-step

1. Open Command Prompt using **Run as Administrator**.

2. Type one of the following commands, depending on your machine:

Windows 7, 8, 10: `tracelog -file \\localhost\perfmontrace.log -maxsize 1000000000 -maxduration 10000000000`

Windows Server 2008, 2012, 2016: `tracelog -file \\localhost\perfmontrace.log -maxsize 1000000000 -maxduration 10000000000`

Where `tracelog` and `\\localhost\perfmontrace.log` are the required files with and name.

3. Press **ENTER**.

The command prompt window displays again after the log file is created.

Perfmon Trace Configuration

Perfmon Trace captures a substantial number records large amounts of information, which can use up a lot of hard disk in a short time period of time. The configuration parameters are available to manage these files.

- **Max File Size:** Controls the maximum number of perfmon trace files for an application. Default = 1 file.
- **Max File Length:** The maximum file size measured in bytes. Default 10000000000 (i.e., 1GB = 10000000000).

Note: These parameters should not be changed without guidance from a Prico representative. Contact your Prico Support representative.

According to the default configuration, the behavior will be as follows:

1. The log file is generated and it reaches a size of 10000000000 bytes.
2. It cannot be created and it reaches a size of 10000000000 bytes.
3. It fails. Fourth and fifth file are created and compressed with flag, until it size of 10000000000 bytes.
4. When the fifth file reaches a size of 10000000000 bytes, the log file is compressed and the cycle begins again.

v17.0 Troubleshooting Messaging Log

The v17.0 Troubleshooting Messaging Log is available to view messages sent via v17.0 MDT using the Messaging Log. You can view the status of outgoing messages, and attempt to resend those that have not been received successfully.

Special configuration is required to enable the Messaging Tool. For more information, see [v17.0 Troubleshooting Log](#) on page 29.

MDT Administration

MDT Administration is used to configure various services for Troubleshooting Manager, Policy Manager, Critical Path Manager, Policy Manager, Configuration, and the Product Manager, as well as perform a variety of management functions of system assets.

General information on MDT Administration is available in the System Configuration Guide and Administration User Guide.

CMA Proxy

This app is used to test CMA proxy code driver connectivity. For more information, see [Device Drivers](#) on page 25.

v16.0 Product-Force Tool

As Product-Force is used to test hardware activity.

v16.0 Proxy

This app is used to test MDT driver connectivity. For more information, see [Device Drivers](#) on page 25.

Activity Log & Diagnostic Tools

PostgreSQLTools.html

PostgreSQLTools.html

The PostgreSQL Tools Check can be used to verify that the PostgreSQL tool setup properly installed and configured, and to diagnose problems. This tool is described in the PostgreSQL

PGSQLTools.html

The PostgreSQL Tools Check also covers up the PostgreSQL Tools Check can be used to verify that the PostgreSQL tool setup properly installed and configured, to diagnose problems and to address that any report errors. This tool is described in the PostgreSQL

Managing Key

You can use Managing Key to check that the network message stored in the PostgreSQL are stored correctly.

PostgreSQL Services Diagnostic

The PostgreSQL Services Diagnostic tool as well as advanced diagnostic options for troubleshooting.

- PostgreSQL Services Diagnostic capabilities table
- PostgreSQL Services Diagnostic Diagnostic capabilities table

PostgreSQL Services Logging Capabilities

Each of the PostgreSQL Services has a set of logging capabilities, among other things, controls the amount and location of logging information. The PostgreSQL Services of the PostgreSQL Services includes the following table, which can be configured for logging in the PostgreSQL Services log directory, the PostgreSQL Services log directory, or both.

- Control Log
- Log
- Logging

- Information
- Setup
- Test Setup

All of these main categories are available in the web console. The **Setup** category is subdivided by enabling or disabling the main activities for the Flow Audit Service.

Log to a Flow Audit Service Log Directory

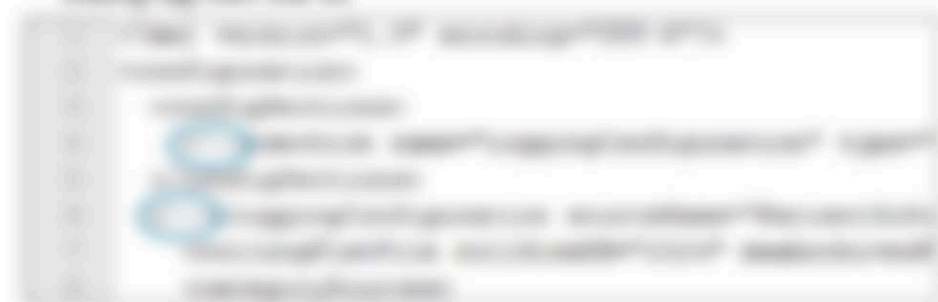
The setting that controls Flow Audit Service logging is called **Log File Destination**, and this is enabled by default for the following reason:

- **Collect Data**
- **Flow**
- **Flowing**

You can add more items to the items listed to adjust the amount of logging by setting the **Log File Destination** of the web console for the items you want to include or exclude.

Setting items to Log File Destination logging

1. Browse to the **Tools > Configuration** page and open the **Tools** for the Flow Audit Service logging you want to edit.
2. Open the web console for logging in test editor.
3. To enable items in the logging configuration, add the **Log File Destination** to the **Log File Destination** and **Log File Destination** page. Add the **Log File Destination** to the **Log File Destination** and **Log File Destination** page.



4. Add the following entry to the **Log File Destination** section for the items you want to enable:

```
Log File Destination: Flow Audit Service
```

Activity 5: Configure Tools

How can I configure logging?

Example: In the example below, critical error logging is enabled with the addition of `critical` to `loggers`.

Example:

```

logging.basicConfig(
    level=logging.INFO,
    format='%(asctime)s %(levelname)s: %(message)s',
    filename='logs/app.log',
    filemode='a')
logging.info('Application started')
logging.error('Application error')

```

1. How can I enable the web logging file?

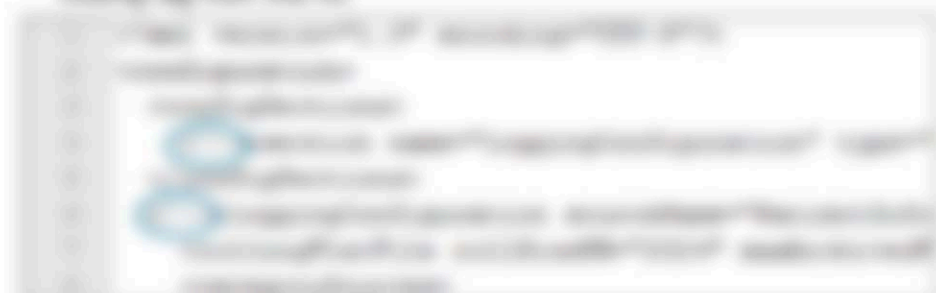
The log file is created in the following location:

The log file is created in the following location:

The log file is created in the following location:

Enabling error logs for the application logging

1. Access the file `logging.py` and open the file for the Python logging module.
2. Open the web logging file using a text editor.
3. To enable error in the logging configuration, add the `error` to the `loggers` list and change `level=logging.INFO` to `level=logging.ERROR`. And add the `error` to the `handlers` list and change `level=logging.INFO` to `level=logging.ERROR`.



4. Review the following code in the `logging.py` file for the module you want to enable:

```

logging.basicConfig(
    level=logging.INFO,
    format='%(asctime)s %(levelname)s: %(message)s',
    filename='logs/app.log',
    filemode='a')

```

- 8.** Please add notes for each coding file.
The key file is located in the following location:
- All cases will represent separate cases throughout the flowcharting
process - all cases will be separately reviewed

Log in to Microsoft Office Word Application

Microsoft Store: Please logging in another way. There are two more links available for logging in the Store: [Store](#) and [Store](#).

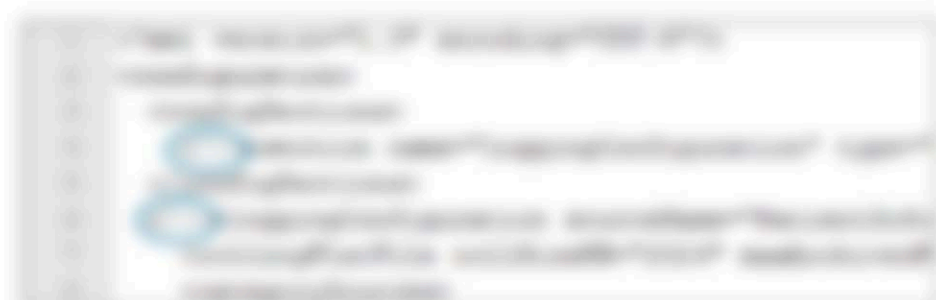
The rate will have impact on various levels to allow the amount of logging by setting the number of the user using the for the user can used to estimate a solution.

The use and control of the system is the Director's responsibility and is not to be used for any other purpose. The system is not to be used for any other purpose.

1. Browse to the `src/infrastructure` and open the `lib/infrastructure` directory. Remove `logging.py` and add `__init__.py`.
2. Open the `__init__.py` file using the editor of your choice.
3. To enable access to the logging configuration, add `log` to the `__all__` list. The logging `__init__.py` will contain `log` and remove the `logging` subpackage. Add `log` to the `__all__` list, corresponding to the `log` subpackage.

Activity Log & Diagnostic Tools

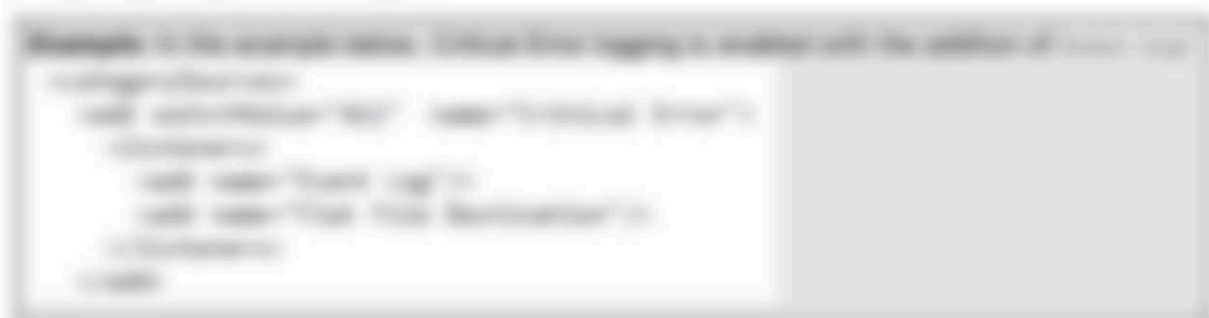
How to Use Service Diagnostic



6. Add one of the following entries in the `...` section for the service you want to enable:

```
user@hostname:hostname
```

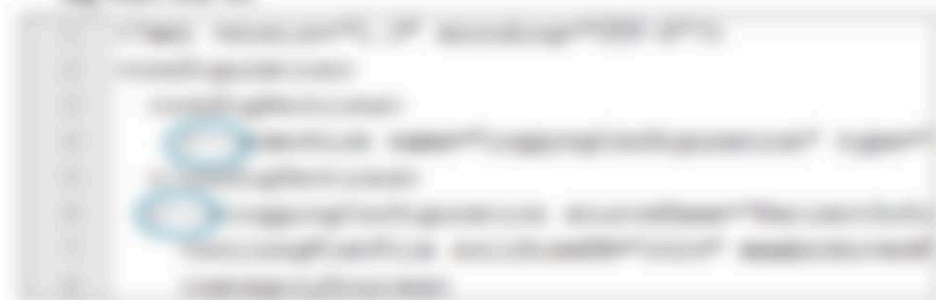
```
user@hostname:hostname
```



7. Save and close the window by:

Setting user for host time logging

1. Browse to the folder `C:\ProgramData\...` and open the folder for the Host Time Service logging you want to edit.
2. Open the user entry file using a text editor.
3. To enable user in the logging configuration, add the `...` section for the logging `...` and change `...` to `...` and remove the logging `...` from the `...` and corresponding `...` by that line.



8. Add or remove one of the following entries in the `...` section for the service you want to enable:

Firewall Service Diagnostic Logging Capabilities

Log Firewall Service Web Service

To troubleshoot problems related with the Firewall Service, a log file can be enabled to capture the Web Service that the Firewall Service sends to the database. When enabled, a log is written to the Microsoft Event Viewer at the Information level. You can change the level to either Debug or Information in the web-config file.

By default, Web Service logging is disabled. If Web Service logging is enabled, it should be disabled again after troubleshooting is complete. The log will also be cleared from the Event Viewer.

Enabling Web Service Log

1. Browse to the folder "C:\inetpub\wwwroot\" and open the folder for the Firewall Service logging web root in web.
2. Open the web-config file using a text editor.
3. Under the <system><logs> section, configure the <add> element as follows:
`<add name="FirewallServiceWeb" source="http://>`
4. Save and close the web-config file.
5. To access the log, open the Event Viewer and browse to Windows Logs > Application. By default, the Web Service log are listed at the Information level.

Configuring Web Service Logging Options

1. Browse to the folder "C:\inetpub\wwwroot\" and open the folder for the Firewall Service logging web root in web.
2. Open the web-config file using a text editor.
3. Under the <system><logs> section, configure <add> element as follows. Be sure one of the following values:
`<add name="FirewallServiceWeb" source="http://>`
`<add name="FirewallServiceWeb" source="http://>`
4. Save and close the web-config file.

Enabling Web Service Log

1. Browse to the folder "C:\inetpub\wwwroot\" and open the folder for the Firewall Service logging web root in web.
2. Open the web-config file using a text editor.
3. Under the <system><logs> section, configure the <add> element as follows:
`<add name="FirewallServiceWeb" source="http://>`
4. Save and close the web-config file.

Log Flow Control Service Request Responses

To troubleshoot potential issues with the Flow Control Service, a log file can be enabled to track and store Flow Control Service requests in a structured manner. When enabled, a log is written to the Microsoft Event Viewer at the information level.

By default, request response logging is disabled. If request response logging is enabled, it should be disabled again after troubleshooting is complete. The log will also be deleted from the Event Viewer.

The log that is enabled includes the following sections:

- **Request:** The name of the service interface method called and the time it took to process the call (in seconds).
- **Request:** Request payload of the message sent to the service.
- **Response:** The data sent back to the requester.

Enabling request response log

1. Browse to the folder "C:\ProgramData\Microsoft\FlowControlService" and open the folder for the Flow Control Service logging log with its sub.
2. Open the web config file using a text editor.
3. Under the `<system>` node, update the `logRequestResponse` attribute as follows:
`<logRequestResponse value="true" />`
4. Save and close the web config file.
5. To activate the log file, open the Event Viewer and browse to **Windows Logs > Application**. By default, the request response log will show at the information level.

Disabling request response log

1. Browse to the folder "C:\ProgramData\Microsoft\FlowControlService" and open the folder for the Flow Control Service logging log with its sub.
2. Open the web config file using a text editor.
3. Under the `<system>` node, update the `logRequestResponse` attribute as follows:
`<logRequestResponse value="false" />`
4. Save and close the web config file.

HL7 Outbound Messaging Log

Messaging Log Overview

The HL7 Outbound Messaging Log (Messaging Log) allows you to view the status of outbound messages sent via HL7v3 and is available at the HL7 server and applications where virtual router applications are installed. The log helps to address messages that being sent if they are not received successfully. Message status is displayed to you from whether an attempt is not a message is successfully received by the external system. If an error occurs, you have the ability to retransmit the record and resend the message.

The status of outbound HL7 messages sent via the Connectivity Manager (HL7v3) can be viewed in the virtual router application either as a notification from the members of whether or not the message has been accepted. The message status can be viewed and messages can be managed through the HL7 Outbound Messaging Log.

Note: To view the status of a message using the HL7 Messaging Log, users must have Diagnostic Privilege.

Messaging Log Configurations

To enable the HL7 Outbound Messaging Log, you must configure both the Messaging Log and each member for which you want to log messages.

To enable and configure the message logging, follow the instructions in the System Configuration Guide to set the logging settings in the PSMC module on each controller. The settings must be added to the configuration files in the `/etc/psmc` directory on each controller.

For more information on using the Configuration Editor in Customer, see the System Configuration Guide.

1. Add a new member named "Management" to the PTOB, with the goal to configure to use standard PTOB.

Property Name	Type	Description
enabled	bool	Activates the interface for message logging. True: Messages sent from this ThreadID will be logged in the Message Logging tool. False: Messages sent from this ThreadID will not be logged in the Message Logging tool.
enablePerformance	bool	Enables the performance monitor. It only applies if parameter RecordFlag. True: Only messages that failed are logged. False: All messages sent from this ThreadID, either successfully or with errors, will be logged.
maximumLogSize	int32 or null	Limits the number of times the interface has to repeat a message in the log. If the parameter is not defined or its value is lower than or equal to 0, the interface will try to repeat the message if any error occurs. If the parameter value is greater than 0, the interface will try to repeat it any error the number of times defined in the value.

Example Below are the three sections in the Configuration Editor window:

Log	Log	Log	Database	Database
SQL	SQL	SQL	Database	Database
SQL	SQL	SQL	Database	Database

Note When configuring multiple interfaces for message logging, you can log a message to different users. When this is enabled, logging is also enabled for each interface. You can also select multiple log user sets. For more information on using the Configuration Editor in Customer, see the System Configuration Guide.

Configuring the SQL Database Managing Log

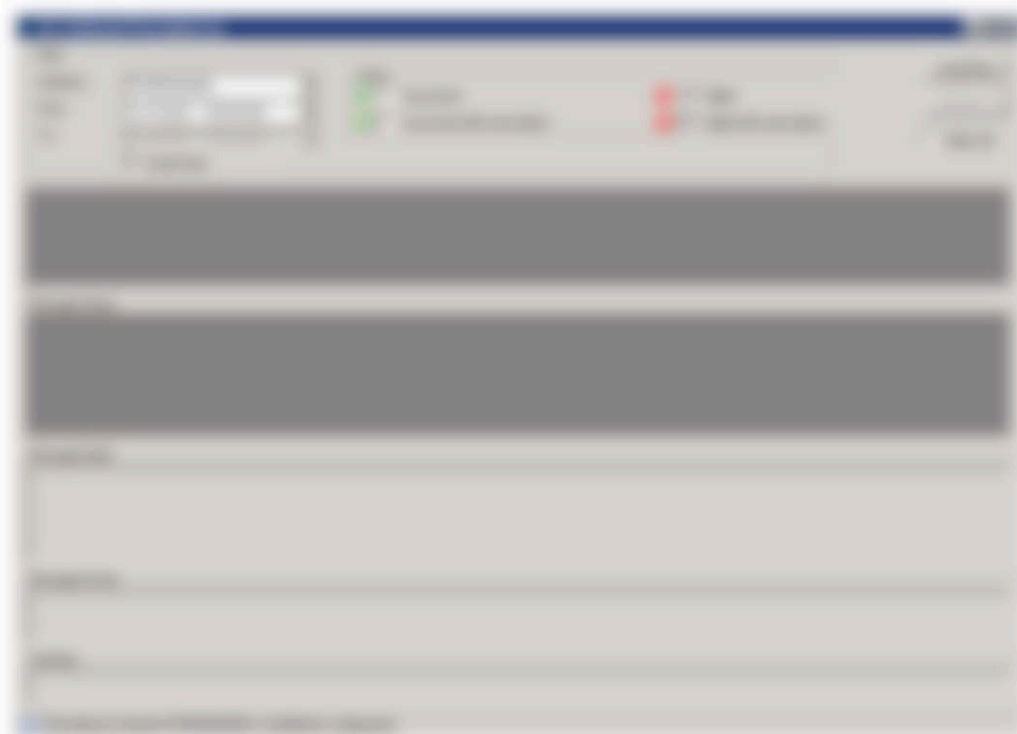
The following settings are configured in the Configuration Editor in Customer Manager: Manage a Field in the Message Managing Log. Select and configure these settings as desired:

Setting	Description
message_enabled	When the Managing Log is opened, the message flag is set to the value is default.
message_log	When the Managing Log is opened, the message flag displays the message default in the user.
message_log_enabled	When is selected, the message should not be any SQL message log flag.
message_log_enabled	When is selected, to check if custom field message is available in log.

Load Interface Database Message Log Data

The Managing Log displays database message data based on these, which allows the user to message to be stored. There are default filter settings, but you can also add the filter to remove or include the stored message.

Note To view the status of a message using the Managing Log, users must have privileges that apply.



Using Bulkmail Management Tools

1. Browse to one of the following locations and double-click the file `FileTools\BulkmailManagementTools` to open the Bulkmail Management Tools.

Source: `C:\ProgramFiles\`

Destination: `C:\ProgramFiles\Thunderbird\`

2. Type your user name and Password to log in and click **OK**.

The `FileTools\BulkmailManagementTools` opens.

3. Click the **Messages** tab and choose the messages for which you want to view bulkmail messages.

Note: The Bulkmail Management Tools are configured to default to a specific interface. The user interface will automatically be the Bulkmail Management Tools in the previous step.

4. Click **Import** to select the data and select **File** to import the bulkmail messages you want to add.

The user interface will show the **File** tab. See `FileTools\BulkmailManagementTools` in step 5.

5. Click the **Import** **File** button.

The messages appear in the **Import** **File** section. Select all your files.

The messages are imported based on when they were sent. The user interface shows the **Import** **File** section and all messages added to a particular account are visible. When a message is selected

In the SQL tool, the Message History, Message Detail, and Message Detail sections are provided.

For more information on these sections, see [SQL Server: Database Managing Log Results](#).

Note: If any of the stored logs changes, a message appears warning that the data displayed may be out-of-date in the current view. To apply the new data, click [Load Data](#).

Review Database Managing Log Results

The managing log is loaded into a section called [SQL tool](#), which shows the filter section. Database section provides more detail about the message and its status.

SQL tool

The SQL tool displays messages that used the SQL engine. The following columns display information associated with each message in the SQL tool:

- Index** - Index of the of the database message for details on message details and message details. (See [SQL tool](#) on page 10)
- Time** - Description of the message and time. (See [Database Message Detail](#) on page 10)
- Message Time** - Description of the message and details and. (See [Database Message Detail](#) on page 10)
- Message** - The message that was sent.
- Message Time** - Date and time when the message was sent for the SQL tool. (See [Database Message Detail](#) on page 10)
- Process ID** - Unique system identifier (SPID).
- Process Name** - Process name or setting in Configuration table (SPID = SPID = Process = ProcessName).
- User Name** - User name of the user who sent the message for the SQL tool. If the message is sent for the message, it will be "SQL" (Process Name or Name or setting in Configuration table (SPID = SPID = Process = ProcessName)).

Message History tool

When a message is entered in the SQL tool section, the history of the message appears in the Message History section. The message history includes the details of each time the message was sent.

The Message History grid displays one of the following columns:

6.7 Outbound Messaging Log

Learn how to view Outbound Messaging Log.

Status	Description
	Successful message sent successfully
	Failed message sent failed

After the filter, the following columns display information associated with the message in the Message Filter grid:

- Time**—Description of the message when sent (Supports Message Filter on page 10)
- Extended Time**—Description of the message when status sent (Supports Message Filter on page 10)
- Message Time**—Date and time when the message was sent (filterable column)
- ACK Message Time**—Date and time when the Acknowledge Message was received (filterable column)
- User Name**—The last name of the user who sent the message. If the MMSB interface sent the message, it will be "MMSB". The listing is sorted in ascending order in setting in configuration (Order Select = Select = Name = First/Last)

Message Detail and Message Status

The Message Detail section displays the entire MMSB message for use that is currently selected in the Message Filter grid. If an MMSB message exists in the selected outbound message, it appears under the Message Status section.

Summary

The Summary section displays information about the filter conditions that are applied and the message count based on filter.

Filter Outbound Message Log Results

The Messaging Log results can be filtered based on the interface name, date range, and message status.

Interface Name Filter

Each message is displayed based on which interface is selected. Each time a new interface is selected, data is loaded in the grid based on that specific interface.

The interface drop-down menu includes the list of MMSB interfaces that have been configured for message logging. For more information on configuring an interface for message logging, see configuring an interface for message logging on page 10.

Time Range Filter

Messages are displayed based on the time range that is specified. By default, the "From" time is set to 1 hour before the current time. You can change this as needed. Messages are displayed based on the current time as the "To" time. To update the filter, select the current time box and specify a new "To" time.

Message Status Filter

The Status option filters messages based on the status you want to see. Messages are only displayed if they match the Status criteria you specify. Status is a summary of the outcome.

Status	Description
	Successful message sent successfully
	Failed: error from the message web with the communication provider failed
	Successful with exceptions: the log from the message web was successful, but other data in the history failed
	Failed with exceptions: the log from the message web was failed, but other data in the history was successful

By default, the filter is set to "Failed" and "Failed with exceptions," so only messages with errors are shown.

Note: The dashboard will automatically update after Status thresholds are selected in Settings.

Review Failed Outbound Messages

MSF-based modules that are configured for message logging can record message automatically if you can record them manually.

Configuring a module to Record Messages

To allow other modules to record their record attempts, the following entry should be added to the `lib/config/Configuration/Parameters` module file:

6.1.1 Database Management Log

Access Point Database Management

enable_db	yes
enable_db_debug	yes (yes: yes, no: no, no default)
enable_db_log	no

The setting controls the database settings. The Management Log only records messages for the Access Point database defined in the subject log. An database setting parameter is defined as:

```
enable_db=yes enable_db_debug=no enable_db_log=no
```

Notes

- enable_db=yes: In the case of the PDB that Support interface.
- enable_db_debug=yes: PDB is debug mode when the PDB interface is tested.
- enable_db_log=yes: Support PDB log.

To configure more than one interface, each configuration must be repeated as:

```
enable_db=yes
```

Example

```
enable_db=yes enable_db_debug=no enable_db_log=no enable_db_log=yes enable_db_log=yes
enable_db_log=no enable_db_log=no
```

Access Point Database Management

- Configure the `enable_db_log` configuration setting. For more information, see [Configure the interface log storage settings in table 15](#).
When a message is successfully stored, an acknowledgment is received and the record storage ends.

Access Point Database Management

- In the Web GUI, click to select the management log that is stored.
To record all of the messages, click the **Record All** function under the Log Data column.
- Click the **Record** button.
If the selected interface is configured to allow recording messages from the application, after the messages are selected, the Record Message confirmation window appears.



6. Click **Send** to resend the message.

When the application attempts to resend messages, they are sent to the FHIR interface and to the web environment only. When a message is resent to either web, FHIR, and FHIR-Web, columns are updated in the table grid.

The following table displays the status of the message:

Status	Description
	While the message is being sent.
	The message was not delivered to FHIR or the operation failed on the server or a configuration parameter.
	The message was sent successfully.
	The message was sent with error.

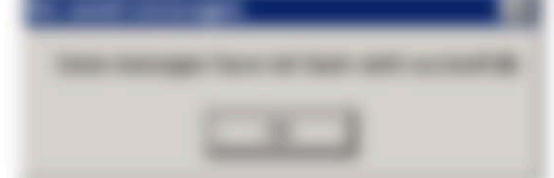
Canceling a Message in Progress

- Click the **Cancel** button while the process is being done.

Messages sent before the cancel action cannot be undone. If FHIR has received them, they will be visible.

Troubleshooting the HL7 Outbound Messaging Log

The following are messages that may be received during the error reporting process:

	If the M/T interface is not configured to allow warning messages, the message will be displayed in the Status Bar.
	In the event that the M/T interface is not available, the message will be displayed in the Status Bar.
	If the connection with M/T server is broken, the message will be displayed, and the message will disappear after the disconnection will not be sent to the M/T interface.

Supported Message Errors

The following are message errors supported by the M/T interface. Any other possible errors will be tagged as "Unknown".

- **Err Error 00:** An error occurred during communication.
- **ErrInterface 01:** The M/T did not send up M/T message and the M/T interface is configured not to send for an M/T message from the M/T.
- **Err Error 01:** The M/T interface received a negative M/T result.
- **ErrInterface 01:** The system sent a negative M/T, which specifies an application-level error (e.g., "Data already processed").
- **ErrInterface 01:** The system sent a negative M/T, which specifies that the user system has rejected the entire message.
- **Err Error 02:** The M/T interface received a positive M/T with some error.
- **ErrConfiguration 01:** The M/T interface has a custom M/T message set in the configuration file and the received M/T message does not match the configuration.
The custom M/T message configuration parameter can be edited via Configuration Editor in **Customer M/T - M/T interface using - M/Communication - M/Personalized communication**.
The parameter is described by **idmmt**, which must always activate if needed.
- **ErrInterface 01:** The M/T interface did not receive the M/T message in the expected time.
Each M/T interface has its own acknowledgment timeout, which can be edited via Configuration Editor in **Customer M/T - M/T interface using - M/Communication - Acknowledgment**.
- **ErrInvalidFormat 01:** The acknowledgment message sent by the user system is not well formed.
- **ErrInvalidID 01:** The acknowledgment message ID does not match the ID of the message sent by the M/T interface.

SQL Database Manager Log

Establishing the SQL Database Manager Log

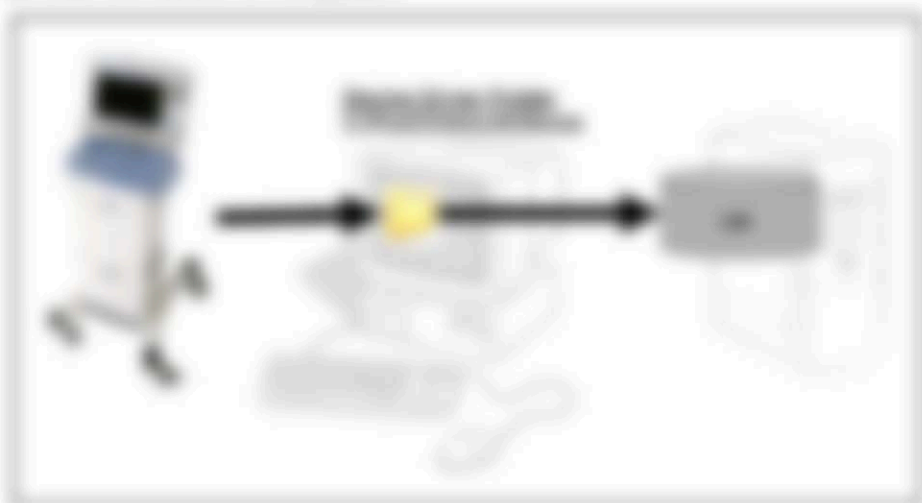
- **Event 25:** A TSPB was received using the communication.
- **ConnectFailedConnection (7):** The user can connect when the local network system starts a connection.
- **ConnectConnectFailed (25):** The connection was unexpectedly broken.
- **ConnectFailedConnection (25):** The user could not be added to establish the connection.
- **ConnectConnectFailed (75):** The user has the TSPB interface is trying to connect to address. The user can't be set as official members of data.
- **ConnectFailedConnection (75):** could not establish a connection to the user system.
- **Internal Error (25):** some other error not specified by the TSPB implementation.

Device Connectivity

Device Connectivity Overview

This chapter presents information for connecting medical devices to hospital workstations with Healthcare Storage. **Health Storage** is critical care storage enabled.

Healthcare Storage, **Health Storage**, and critical care storage collect device data from medical devices connected to the system.



Workstations with **Therapeutics** and critical care applications enabled are connected to medical devices via a secure connection. For each connected medical device, a corresponding device driver is installed on the workstation. The device driver is responsible for interpreting the raw data received

NOTE: This does not stop creating any HTML content and content, all you find information available in this document.

[illegible]

Medical Device Implementations

The following recommendations and issues are based on implementation experience. If you have any questions please contact your PACE representative.

Recommendations

Cable Coding System

Consider a cable coding system for all connections with medical devices.

- Set up a code for each type of medical device to be connected to Physiotherapy and Medical Data applications. For example, use code for ventilation and a different code for patient devices.
- Color code cables needed for each medical device.
- Color code ports that connect to the device.
- Include color coded symbols for color-coded ports.
- Document the color and place signs close to the applications or device.

Note: A cable coding system can not be used with serial expansion.

Cable and Connections

Device requirement for connection cables:

- Tie loose cables together to avoid tangling, noise and safety coding.
- Use high quality communication/connection connections.
- Device replacement cables and connections are available in case of failure.

Modem Issues

If you are using a modem and need it with coding included:

- Set up all coding from modem modem wires.
- Use ports in sub-modem wires for their connection to medical device.

Serial Expansion Connections

Device serial expansion connections to computers:

- No connections to prevent unwanted serial disconnections.
- Device cables are needed to serial expansion about specifications. These are specific to the manufacturer and not provided by PACE. All specifications provided by PACE are for connecting directly to a sub-modem.

Testing and Debugging

After successfully installing and configuring the device and firmware, testing that updated versions of the device will be sent to you by Flex. If enhancements are required.

Potential Hardware Issues

As you are installing and configuring device connectivity, you may experience some of the following issues:

- Medical device incorrectly configured communication ports settings. Medical incorrectly configured, installed incorrectly, or connected to the wrong communication ports path.
- Cable incorrectly connected (wrong or cable). Device connection, incorrect connection to device or cable connection.
- Serial number ports connected.
- Serial number incorrectly configured.
- Wrong cable used for a specific device.
- Cable connection made due to a tight connection.
- The medical device does not support serial communication. An error setting needs configuring to the device manufacturer.
- Device connected with incorrect device driver loaded by the Plug-and-play and Virtual COM application.

Practical Examples

The following provides some common example configurations of medical devices.

Note: This should be used for guidance and information purposes only.

The screen highlights the specific details.

Media Area with Hidden Computer

The media area contains and hides the tablet. The computer is positioned behind the wall.



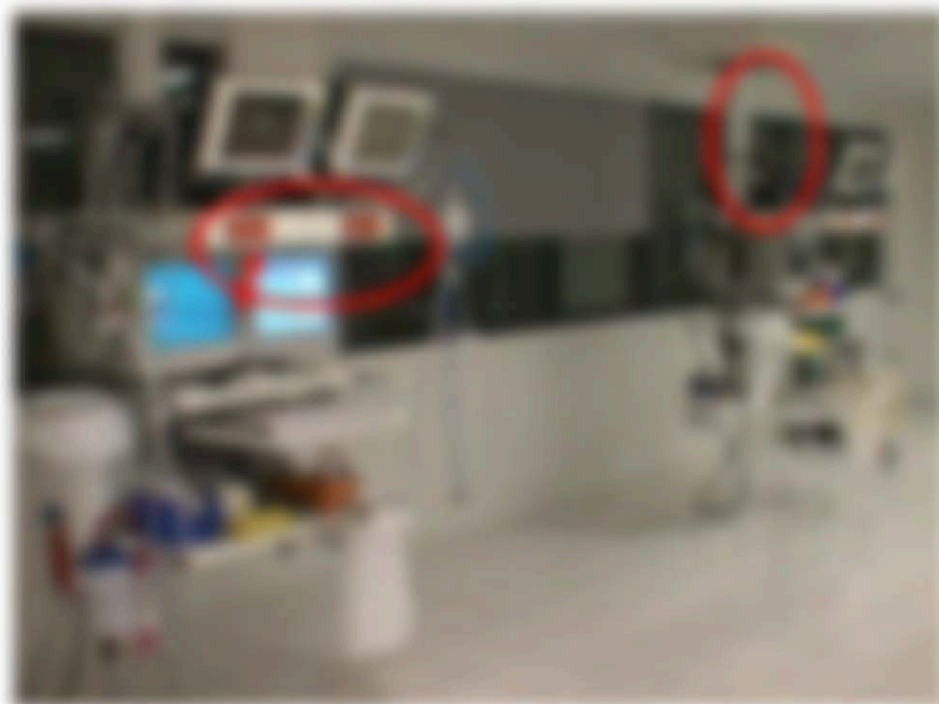
Mobile device with cables protected

The mobile unit connects and holds the cables. The computer is positioned against the wall.



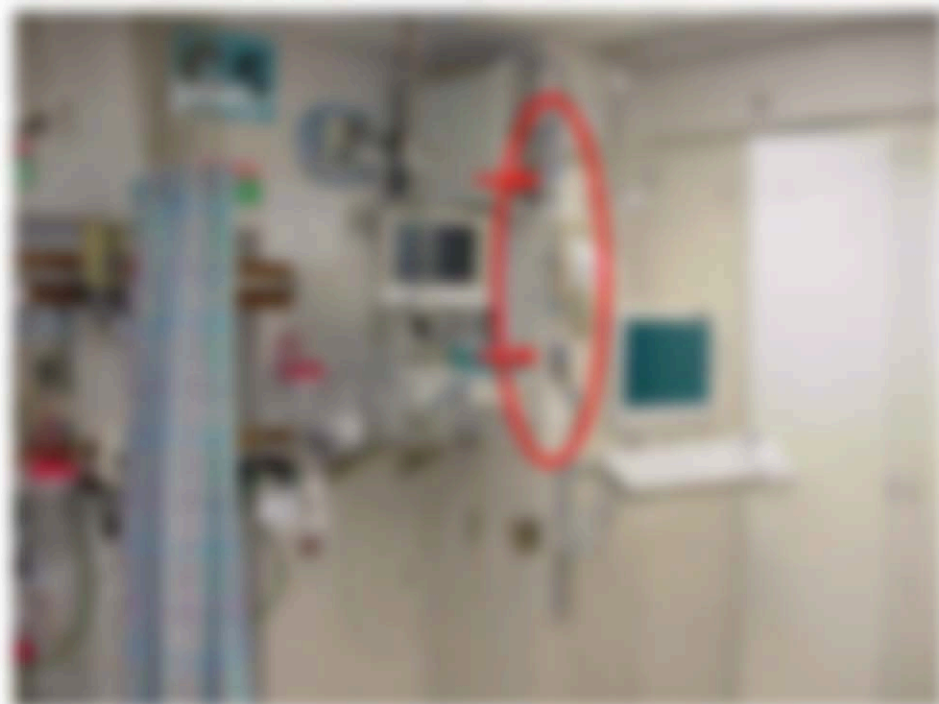
Standard Configuration for mobile devices

Mobiles are configured with standard ports and devices are mobile devices can be attached



Registering Devices

Devices are registered to avoid conflicts with system calls



Device Drivers

Device drivers are developed using two complementary technologies. The following table shows the differences between these methods.

Method	Traditional	New Device Technology (NDT)
Architecture	Uses the user API	Architecture directly with the kernel
Devices Supported	Physiomedical devices for example: Ventilators, monitors and infusion pumps	Physiomedical devices for example: Ventilators, monitors and infusion pumps, infusion pumps with fluids
Programs Used	Kernel user API	NDT API

Attribute	Chakra Core	New Device Technology (NDT)
Device Identification	Identifies device driver files that will be in the package.	Identifies device driver files that will be in the package (NDT 1).

Device Driver Contents

Device drivers are distributed from the setup package as the files that contain the following files:

File	Description
File	The binary code which implements the data structure from the installed device.
File (File.inf or .cat)	File for which contains the setting specifications, device variables and any special usage instructions.
Configuration File	Device driver requires use of one of these files to determine variable or communication settings. Hardware File - Hardware Device Hardware File - Hardware Device (only, Hardware File, etc.) Hardware File - Hardware File
Hardware File	The file contains a short description of the changes introduced in each driver version.

Installing a Device Driver

Drivers for installed devices are available or required from the File Manager.

Installing a Device as a Peripheral

1. Double-click the device driver file.
2. Select the file in "File Manager" folder (Device File).

Note: Device driver requires additional installation steps. These will be explained in detail by the File Manager.

Installing a Device Driver using Chakra Core File

Note: Chakra Core device driver requires use of a file.

1. Open File Manager (File Manager) or File Manager (File Manager).
2. Select the file in "File Manager" folder and double-click the file (File Manager).

Device Connectivity

Troubleshooting Device Drivers

Note: You will need the Diagnostic Tools system right to open the Troubleshooting. See your Flex system administrator if you do not able to open the Troubleshooting.

1. From under Device Driver, select a driver you want to test.
2. Under Setup Flex, select the setup path to which the device is connected.
3. Click **Test**.
4. Click **Stop** to end the process.

Testing a driver using WFFlex

Note: WFFlex device driver cannot test with a file.

1. Under Hardware Storage, click Storage, or Virtual Tape Storage.
2. Browse to the WFFlex (Physical Flex, virtualFlex) node and double-click the WFFlex icon.

Note: You will need the Diagnostic Tools system right to open WFFlex. Contact your system administrator if you do not able to open WFFlex.

3. From under Device, select a driver you want to test.
4. Under Flex, select the setup path to which the device is connected.
5. Click **Test**.
6. Click **Stop** to end the process.

Interpreting Device Driver Diagnostic Tools

Each diagnostic tool record raw data and decoded data. Raw data is displayed in the format that is received from the device whereas decoded data is data as it will be displayed in the application.

Troubleshooting Device Drivers

Device driver troubleshooting is divided into two steps:

- **Hardware:** Physical connection problems occur between the workstation and physical device drive. In the Diagnostic Tools, no data will be visible in the Raw Data window. See Troubleshooting issues on page 25 for a list of possible issues.
- **Software Driver:** There might be an issue with the device driver used. The following are possible issues:
 - Wrong version of the driver might being used. See Troubleshooting device driver on the previous page for information about troubleshooting the driver version of a drive.

Device Connectivity

Device Data Stored in the Database

Note: You will need the **Diagnostic Tools** system right to open **File > Open File**. See your PDA system administrator if you do not able to open **File > Open File**.

1. From under **Device Group**, select the device you want to view.
2. Click **View** and open in **Source File**, enter path and filename of the file to be viewed.
3. Click **OK** when you have finished.
4. Click **Next**.
5. Use the arrow keys at the bottom of the window to navigate through data collection points.

Setting a log file using WDT file

1. Open **Procedures Manager**, **Procs Manager** or **Global Proc Manager**.
2. Browse to **C:\Program Files\allsoft\wonder** and open the file **WDTFile.exe**.

Note: You will need the **Diagnostic Tools** system right to open **WDT File**. See your PDA system administrator if you do not able to open **WDT File**.

2. From under **Device Group**, select a device you want to troubleshoot.
3. Click in **Source File**, enter path and filename for the file you want to view.
4. Click **Next**.
5. Use the arrow keys at the bottom of the window to navigate through data collection points.

Perfect Trace and WDT Drivers

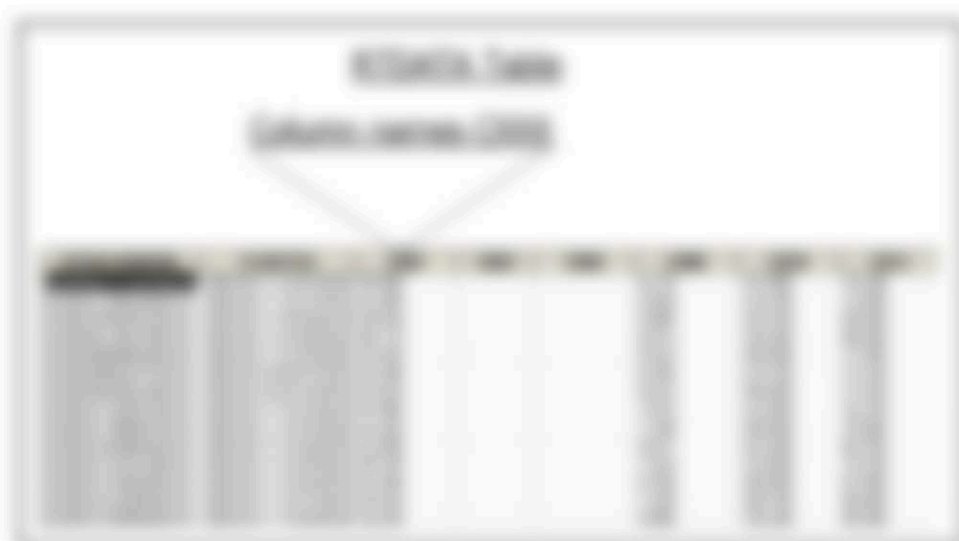
Perfect Trace can be used to log WDT drivers. Perfect Trace stores the system information as WDT file, and additionally application messages. Perfect Trace is used when troubleshooting problems related to application activity, not just the device driver. See **Perfect Trace** on page 23 for more information.

Device Data Stored in the Database

Device data is stored in the database in three tables:

- **WDTDevice** - Stores device data.
- **WDTDeviceAttribute** - Stores device data that is attributed.
- **WDTDeviceEvent** - Stores device data that is captured in a table.

To optimize database storage, in these tables each column represents a different variable. The size of the column is fixed in each table, contrary to the variable. For list of all tables and variables see the **Procedures** - Variables table in the index.



In each database table, data will be stored. Different types of data are stored in the database. When the new service is created, new data is added. The data is added and a corresponding record will be added to the database.

The system workflow is such that the new service is created including the service, a service user, and the service location. The service is added to the database. The service user adds the configuration data, and the system that then adds the service location to the database. In the system, the data is added with the database information, and the data is the information that is added to the database.



Creating a new database column in the HDFS table

This procedure should only be undertaken by a qualified database administrator who has administrative access to the HDFS database. If you are in any doubt contact First Support before proceeding.

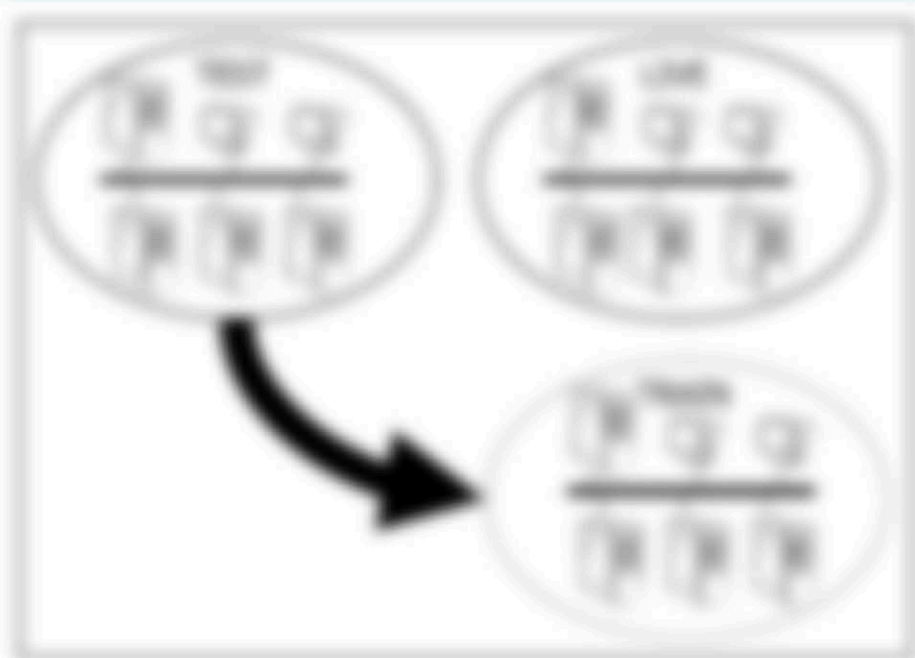
1. Open the Service Management Studio and connect to the HDFS database.
2. Copy and paste the contents of `testHadoopTable.sql`. You only need copy the script for your database vendor.
3. Review the script to ensure all variables to be created are correct.
4. Run the script.
5. Run the following script and check the columns have been added to the HDFS table:

```
SELECT * FROM test
```

6. Review the results to ensure the table now contains the columns added.

Additional Environments

Create Additional Environments



If an additional environment is required, for example Top or Bottom, then use arrows on the existing customer to indicate the transition, upgrade, and support will accept the responsibility of the customer. It is recommended that customers make a copy of their own environment in order to create the additional

Additional Environments

Creating Additional Environments

environments. If the additional environment requires getting it should be recorded by issuing the `get` command.

Note: In addition to `DEV` and `UAT` environments, sites that are already live with one product and want to install additional products to develop a `PRD` system. An example will install a `PRD` environment. `DEV`. The `DEV` environment is used to building the integrated `PRD` system while leaving the `DEV` environment live for troubleshooting and testing the system prior to release. The live site may be required during the time it takes to implement the `PRD` system. The `DEV` environment is only supported by those with the `PRD` system goes live. Then the `DEV` environment becomes the new `DEV` environment and the existing `DEV` environment is archived.

Creating Additional Environments

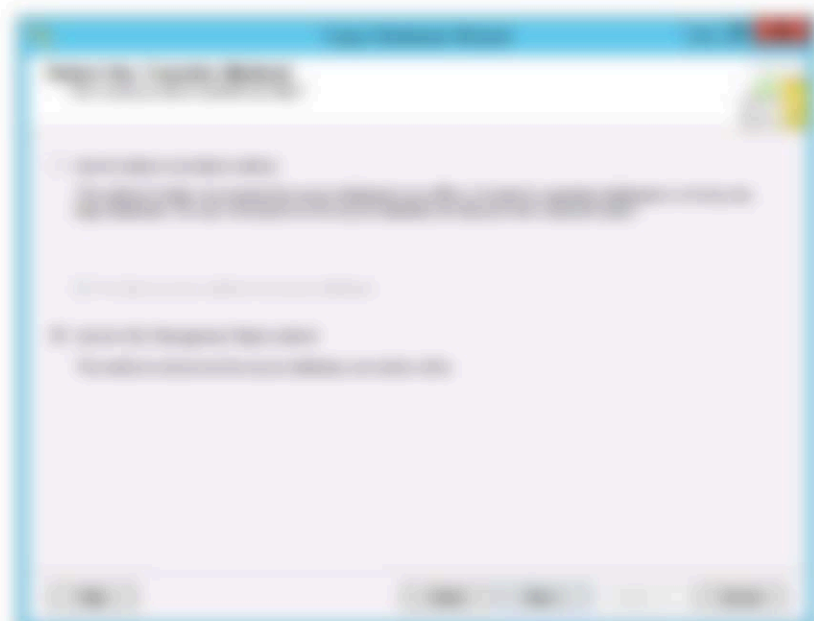
Note: The procedure describes sites documents which are available from the user community at <http://ibm.com/ibm/ibm>.

1. Prepare and configure the database server. See the installation guide for database instructions.
2. Copy the live database. See the procedure Copying, Transferring and Updating Data across Platforms under the **Tools** information.
3. Restore the database. See Copying or Restoring a DB2 Database and Update Data across Platforms under the **Tools** information.
4. Restore the code and scripts. See Copying the code and scripts for Transferring and Updating Data across Platforms under the **Tools** information.
5. Install and configure the application components. See the **Installation** installation guide.
6. Install the management console. See the **Server** installation guide.

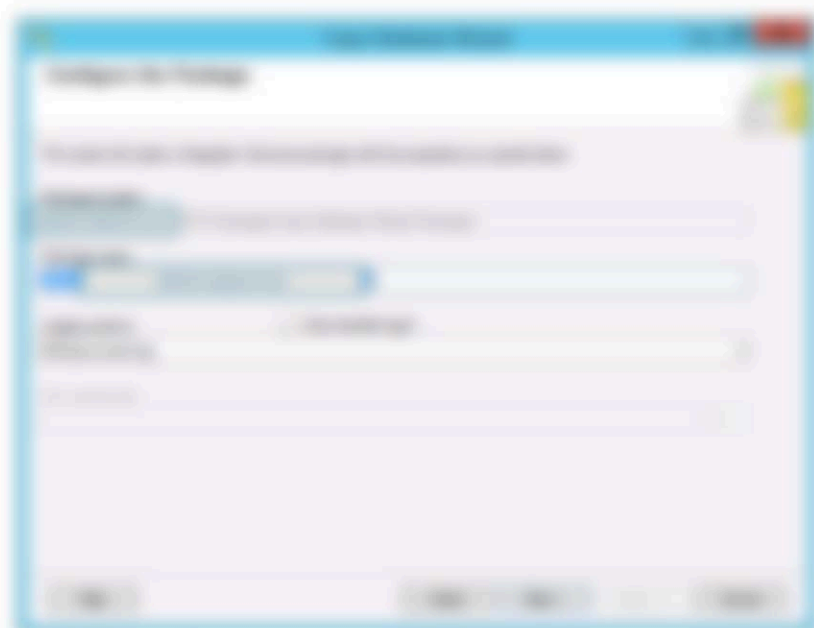
Copying, Transferring and Updating Data across Platforms

The procedure outlines how to copy a database from one server to another server.

1. Before copying a database to a new or existing server, it should be connected to the database. Additionally, all other servers except the database server should be stopped.
2. In the source the database server, start the **DB2** monitor and then open a **Program**.
3. From a **Microsoft SQL Server** monitor and then click **Management Studio**.
4. In the **Connect to Server** window, type the server details and the user name and password. Database details appear in **SQL Server Enterprise Manager** (Server Explorer).
5. In the **Server Explorer**, click to expand **Databases**, under the **SQL Server** instance.
6. Right-click the **Databases** and then click **Tools -> Copy Database**.
The **Copy Database Wizard** appears.
7. Click **Next**.
The **Select a Source Server** window appears.



17. Select **Yes** for the **Yes, Management Agent Method** and **Yes** for **Yes, the Amazon CloudWatch console appears**.
18. In the **Tags** section, select the tag key to each instance in your Amazon EC2 **fleet**. We need to select the **Tag** section and not the **Value** section.
19. Click **Next** when you have finished.
The **Configure Amazon CloudWatch console appears**.



optional, click the settings details. If desired, click **View More**.

The following list describes the Storage settings options:

- **Storage** is the default settings and view More.

If available, if your settings appear. Review your settings to ensure they are available.

- **Storage** is the default settings and view More.

The only item created the rights of the user access to the map provides an error during the storage. This can be easily ignored.

Each item will be copied. After the copy is complete you should review the Storage section to see if there are any red or warning or failed copy of an item. Review the specific item to see if it is a user access issue, which can be ignored, or requires further investigation.

- **Storage** is the default settings.

Setting a database in the Performance and Virtual Host system

The procedure describes how to create a database.

1. From the Database server, click the **Start - Programs - Microsoft SQL Server - Enterprise**.
2. In the Database server window, type the server name and the user login credentials.
3. Open the server. Then click **Tools - Performance - SQL Server - Performance**.
4. Click **SQL** to create the query.
5. Open **SQL** to create **SQL** queries and then use all of the default user access rights to setting all of the locations where the database server is distributed in other locations.

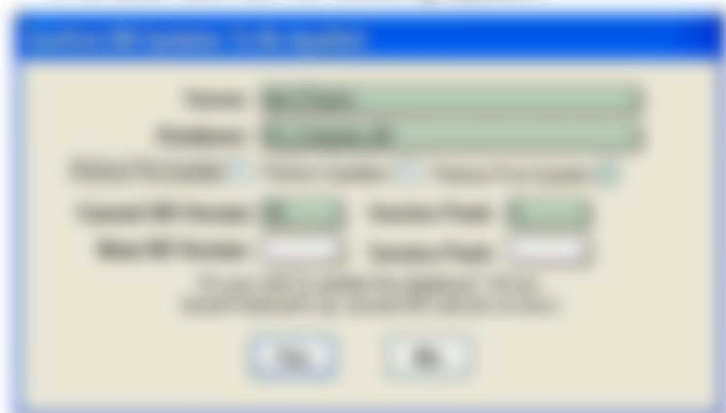
The information on SQL settings, see Appendix B in the Server Installation Guide.

Recording the setup and logins for Postoperative and Critical Care system databases

This procedure describes how to record the Post-Operative and Critical Care database setup and should be performed against all target databases.

DB utility is required. For more information on any of the steps, see the Appendix A in the Server Installation Guide.

1. Start and configure DB utility.
2. Remove the database set of records. (This creates a database set.)
3. Select the database in the system table and click **Update Database**.
A window such as the following appears:



4. Select the **Postoperative** or **Critical Care** record set and select the other fields (table).
5. Click **Yes**.
A window will show the records that will be set against the database.
6. Click **Proceed with the Update**. The installation will proceed.
Respond to the question in the subsequent windows (yes).
7. Click **OK** when the confirmation window appears.

Outlook Booking Appointment Settings

Workflow Overview

Out Manager customers who use Microsoft Outlook can use the Booking Outlook Group settings screen to set up appointments to automatically send out a change booking to the Outlook calendar of managers and administrators.

This chapter shows what happens when the Out Manager is Outlook Calendar feature is set up and working.



Additional Rules for Booking Appointments

There are three sets of additional rules for sending booking appointments to the Outlook Calendar:

- Rules related to the booking
- Rules related to surgeons and assistants
- Rules related to overbookings

Rules for Bookings

The rules related to the booking itself are presented in the table that they are performed in the system:

1. If the **Send Booking Note** box is not checked, do not send the appointment.
2. If the **urgency date** is earlier than the number of days in the **Response window**, then before sending the appointment, the user creates or changes the booking. Do not send the appointment.

Example: If today is Dec 5, 2019, and the response window days is set to 5, and the user is changing a booking with a book date of Dec 5, 2019 to Dec 15, 2019, then do not send appointment.

3. If the booking date is today, and booking time has already passed, do not send appointment.
4. If booking status is either **Rejected** or **Booked**, do not send an appointment.
5. If it is a new booking, send the appointment.
6. If booking date is modified (new booking date), send appointment, except if the date is earlier than the response window time.
7. If using email time is specified and time is changed then send an appointment.
8. If any new surgeon is added to the booking, send an appointment.
9. If any existing surgeon deleted from booking, send an appointment.
- Otherwise, do not send the appointment.

Rules for Surgeons and Assistants

1. If this is a new booking, send a new appointment.
2. If booking status is changed to **Cancelled**, send a **Cancelled** appointment.
3. If a cancelled booking is changed to active, send a new appointment.
4. If a rejected or confirmed booking is changed to active, send an update appointment.
5. If a surgeon has been added to the booking, send a new appointment.
6. If the surgeon has changed, send a **Cancelled** appointment for the old surgeon and a new appointment for the new surgeon. This works for updates as well as single bookings.

Booking Appointment Settings

Calendar Feature Setup

1. If any of the procedures for this calendar has been changed or swapped with another procedure, send an update appointment.
2. If any of the procedures for this calendar has been deleted, send an update appointment.
3. If any new procedure is added to this calendar, send an update appointment.
4. If the booking start time or end time has changed, send an update appointment.
5. If the booking date has changed, send an update appointment.
6. If any existing calendar is deleted from booking, send cancel appointment. Before generating the cancel appointment message, the system will first cancel appointment with cancel comment in the message body.

Otherwise, do not send an appointment.

The following procedure is used to set the Booking Calendar Appointment Settings in the Booking Calendar Management Report, and it is determined that an appointment should be sent. Additionally:

- When generating an update appointment, it checks to see if there was a new or updated appointment added to the calendar or procedure for the booking. If not, it creates a new appointment.
- When generating cancel appointments, it checks to see if there were any new or updated appointments added to the calendar or procedure for the booking. If not, it will not send a cancel appointment, because a calendar has been deleted or appointment for the booking is the first step.

Rules for Appointment Requests

1. If this is a new booking, send a new appointment.
2. If the booking is cancelled, send a cancel appointment.
3. If a cancelled booking is changed to active, send a new appointment.
4. If a requested or confirmed booking is changed to active, send an update appointment.
5. If a booking start time or end time, as defined in the Booking Calendar Appointment Settings, has changed, send an update appointment.

Calendar Feature Setup

Setting up the CRM Manager to include calendar features must be done in three different components of your installation:

- CRM Manager setup
- Invoicing setup
- Booking setup

Outlook Booking Appointment Settings

Outlook Manager Setup

Prerequisites

Before the Outlook Manager Calendar feature can be set up, your site must meet the following conditions:

- Your site must be running Microsoft Outlook as its email software. The feature has been certified to work with the supported Microsoft Outlook versions documented in the Release Notes. The calendar feature is neither guaranteed nor supported for other versions of Outlook.
- Outlook must be installed and running on the same server as Outlook.

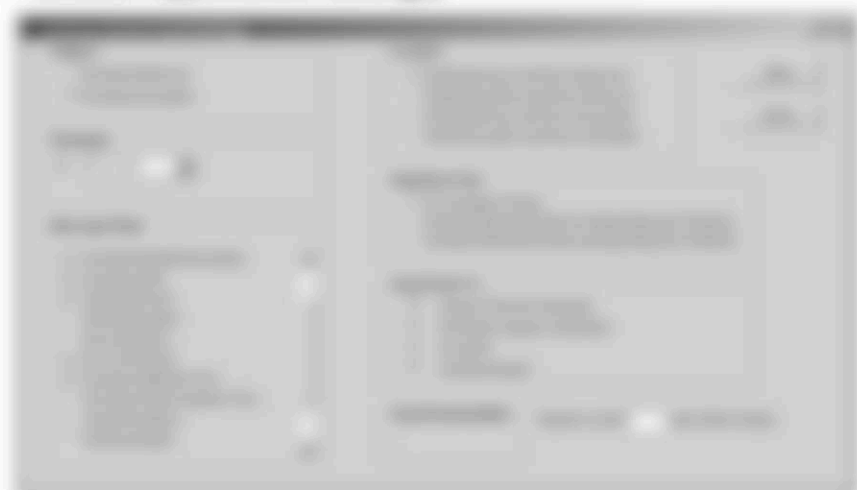
Outlook Manager Setup

After the prerequisites are met, the feature must be completed in Outlook Manager:

- The email address information for each manager and appointment owner whose Outlook calendar you wish to make available for bookings must be in the Manager listbox, and the **Book Email** box must be checked.
The Booking Outlook Email Settings screen must be filled in. See Booking Outlook Email Settings on the next page.

Booking Outlook Email Settings

Outlook Manager creates each appointment's subject, location, and start and end times, and manages each booking. In this step, you set up the Booking Outlook Email Settings screen: **Bookings > Settings > Outlook Appointment Settings**.



1. Select settings in each section to specify how each piece of information should appear in the calendar entry. Check all that apply.

Outlook Booking Appointment Settings

Appointment Setup

Example: Should the subject show the Provisional Appointment in the Provisional Description? What information should be in the message body? How about the location and user details for location?

1. Enter **Reminders**. If you want to have Outlook send a reminder before the meeting. (Then enter the number of minutes, hours, or days before the meeting you want the reminder to be sent.)
2. Enter **New Booking Note**. This sets the custom flag when booking, and it is to enable booking changes to be sent to Outlook.
3. Enter a number in the **Response email**. This allows people who do not respond from getting Outlook calendar appointments, either from the specified number of days before the appointment, unless there is other appointments in the period right up to the day of the appointment.

Autoprint Setup

Prerequisites

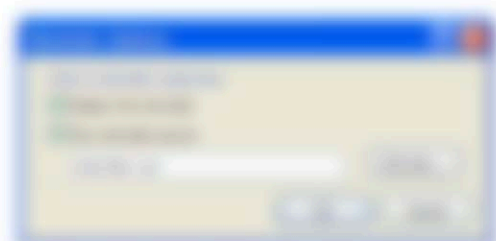
- 1. Microsoft Outlook must be installed on the server where Autoprint is installed.
- 2. An email box should exist in the POP accounts' configuration table. This should have been completed as part of the server installation.
- 3. Create a new Outlook user profile. Autoprint will use this user profile Outlook and send mail. Autoprint should appear in your Outlook's main address book.
- 4. Give Autoprint its own mailbox and Autoprint email only.
See Autoprint on page 32 for further information.

Outlook Setup

1. Create a new Outlook user profile. Autoprint will use this user profile Outlook and send mail.
2. Because Outlook Manager sends appointments from the Autoprint Service, you won't need to add appointments any way to the server. Make sure that you turn off the automatic sync up in Autoprint service through Outlook.

Setting of the Outlook account

1. In Outlook, go to **Tools > Options** and select the **Other** tab.
2. Check the **Advanced Options** button.
3. Check the **Reminders** Options button.
The Reminders Options dialog box appears.



4. Overview for Managing the Appointment Settings

If you use the new Outlook Outlook 2003 security updates (SP1) to the appointment will need additional setup. See Outlook 2003 - Appointment Settings.

Outlook SP1 Background

If you have the SP1 in service with Outlook Outlook 2003 is working when the Outlook application needs an appointment. Because Outlook has to use the user data in the Outlook user data table some changes in the settings for the Outlook Outlook user profile.

Look security settings for the Outlook user and change system settings for Outlook with a file from the Outlook user data. Outlook 2003 Support for Outlook information.

See Information information about the Outlook 2003 security updates at the Outlook Microsoft website (MSDN) for more information on Outlook security updates.

Database Backups

Backup Strategy

The first step is to decide the system backup is required. It is not a copy of all the hardware files, but only the database files. The second option is to create a backup of the system, using a backup utility, and then to restore the system files. The chapter offers recommendations on setting up backups and when they should be.

When planning a backup strategy, there are several components to consider:

- SQL Server hardware
- SQL database
- Server/Network architecture
- Backup hardware

SQL Server Hardware

When using SQL Server redundancy through mirror logging, the system has a copy of all data written to the active server is automatically written to the mirror logging server. When processing for an active server, the mirror automatically writes out the logging or alternating database.

In order to avoid the expense of mirroring, you may opt to have a single active SQL server. When the hardware fails, you restore database backups to the active server and restore operations. The strategy involves using a backup of the active server to the active server, and also restore from the log backup that is available in the active server.

Database Backups

Backup Strategy

SQL Server Database Backups

There are three types of backup jobs that can be configured to help protect data. The backup jobs can be set up at any time using the SQL Server Enterprise Manager. It is using a standard backup implementation used for other database servers in your organization.

Below is a description of the three types of database backup jobs:

- **Full** performed on a specified day and time. Full backups can also run daily, depending on the database size.
- **Differential** performed the number of days after the last backup that you set in the options that specified for full backups. If daily. If differential backups are run hourly, they should not occur less frequently than the hour at which the full backup runs.
- **Transaction** performed hourly, or every 15 minutes or minutes. If differential backups are hourly.

Note: Any backup job that is setup requires that the full backup be configured first.

Note: A differential backup is cumulative — it contains all database changes since the last full backup.

Note: There are requirements for setting up full and backup jobs. It is critical that a backup job be configured and maintained by the job. There will not be data for any event or data that resulting from an implementing appropriate backup, restore, and maintenance procedures and policies.

Setup Backup Jobs

Backup jobs are not automatically setup by their backup installation. They must be setup by the job. This is coordinated with other steps of jobs.

To setup a backup job on jobs, jobs may use the SQL Server Enterprise Manager. It is using a backup implementation the same backup implementation used for other database servers in their organization.

When planning to setup the backup job, you should select a time of day when the backup is best done in relation with server processing.

Note: To ensure enough data jobs for backup recovery, a SQL Server Database that needs must be setup with a scheduling or scheduling to ensure full or. Database that setup is the responsibility of the job.

Note: It is able to select data collected by backup, include using compression. The option can be set at the server level or at backup job compression by default.

Restoring a database

See the [SQL Server help](#) for information on restoring backup files.

1. If the database has crashed, but the log file is still accessible, then back up the end of the log file (the information that was written since the last log file backup was performed). In SQL Server, this can be accomplished by choosing **Backup** | **Full** | **Transaction Log**, and then in the backup page select **Back up the tail of the log**, and leave the database in a restoring state.
2. Restore the full backup.
3. Restore the differential backup if it is the last backup since the full backup.
4. Restore the transaction log backups that were made since the last restored backup which could be a full or differential backup.
Log file backups are performed every time the job runs by default. This frequency can be changed when the job is set up. Doing so, even just decreasing the frequency, will cause slight gaps if possible after the job is set to restore.
5. If you were able to back up the tail of the log with step 1, then restore that backup. Otherwise if possible, repeat the instructions that occurred since the last log file back up.
It is strongly recommended that you test restoring from media created by the backup to ensure that backup files can be successfully restored.

Server/Transaction Processors

Although no critical data is stored in servers and transaction processors you may want to periodically backup or image these machines so that they can be quickly reinstalled following a hardware failure.

Spare Hardware

It is not uncommon to have a hardware component fail after a few years of operation. Consider having spare hardware available.

Maintenance Jobs

Maintenance Jobs Overview

This chapter gives guidance for routine maintenance of your ForgeRock and Oracle Java system. Maintenance tasks include:

- [SMA Server Maintenance](#) in [step 10](#)
- [How and Where SMA Server Services in the Web Page](#)
- [How to Perform Management Service in step 10](#)
- [Configure SMA Server Agent jobs in step 10](#)
- [Customize Reporter SMA Server Agent jobs in step 10](#)
- [How to Configure SMA from the Java JST jobs in step 10](#)
- [Maintenance Schedule in step 10](#)

SMA Server Maintenance

SMA maintenance of your SMA Server consists of two tasks:

- [Installing the server agent log for the SMA Server](#). [Check the help file for your SMA Server version for instructions on installing this log.](#)
- [Installing the event - source application log for the machines on which the SMA Server resides](#). [Check the updating system help file for instructions on installing this log.](#)

Maintenance jobs

Stop and Restart SQL Server Services

Interpret the SQL Server Error Log

Browse through the SQL Server Error log looking for errors. Startup and Transactions errors in the Error log are serious.

Interpret the Application Log

In the first column of the log, you can identify with what action or set of events:

- **Msg** is informational. There was nothing wrong with the event.
- **Msg** is a warning. Double-click the event to see details about the warning.
- **Msg** indicates a critical problem. Double-click on the event to see details about the problem. That event often details a warning about that should be resolved by user IT staff.

Any events in Msg or T-SQL which reference database tables or applications should be reported to your information system staff.

Stop and Restart SQL Server Services

If you need to restart the services, SQL Services need to be stopped and action being to start them again.

Stopping SQL Server services before starting the server

Stop the MSSQLAgent and MSSQLServer services. For instructions on stopping SQL services, please see the Microsoft SQL Server Management Studio help file.

Note: If either of the services does not stop in 30 seconds, restart the server.

Restarting SQL Server services after starting the server

After the server has started, restart SQL Services and address the problems by following the instructions in the Microsoft SQL Server Management Studio help file.

If any problems are shown double-click the problem to see more information or you instead of going through a Service Request. As an expert network expert, or someone who do not do work on the system.

Stop the Microsoft Management Services

As part of routine maintenance or while troubleshooting, it may be necessary to stop a subset one or more management services. The integrated nature of Performance and Central Data collection means that stopping one service may mean other services need to be stopped to maintain system integrity. Use the following table as guidelines when stopping or starting your services.

- **Stopping:** First, recommend following Microsoft's advice of stopping services in a specific order.
- **Stopping the Database Service:** This is stopping the Database Service of other services should be stopped. Users also need to log out.
- **Stopping a Transaction Processor:** This is stopping a Transaction Processor of services should be stopped.
- **Stopping the MIB Service:** This is stopping the MIB service the external systems should stop sending messages.
- **Stopping the Proxy Network Service:** This is stopping the Network Service the external systems should stop sending messages. Users will continue working, but may experience slower performance and will not be able to join their Measurement Storage, Policy Storage, or Central Data Storage.

Important Notes

- From the command prompts or scripts are stopped, monitor logs to be aware available in Proxy, Performance and Central Data applications and they are monitored, after which a alert time is sent up. The logs describe the status.
- If only the application service needs to be restarted, then only the jobs in that application service need to be stopped.
- If the MIB Service is to be restarted, then you need to follow all of the steps in this topic.

Stopping management services

The procedure uses the task environment from the Database Service Configuration on page 11-48 as follows:

1. Ensure all users are logged off all Performance and Central Data applications.
2. Stop all external communications from the external systems (MIB, Storage Management and Validation, systems etc.).
3. Stop the service hosting MIB.
4. Stop the Proxy Network Service.
5. Stop Message and rule sets send messages.
 - From the task bar double click the Taskbar icon show hidden.

Requirements table

How to install Management Server

1. Click the **Yes** next to **SetupServer.exe**
2. Stop the server hosting IIS/MSIS
3. Stop IIS/MSIS and add the user manager
 - From the user manager add the user manager user (see below)
 - Click the **Yes** next to **SetupServer.exe**
4. Stop the server hosting IIS/MSIS
5. Stop the IIS/MSIS Server
 - In the Windows Task Bar -> double click the IIS Server icon 
 - Click on **Server** - select the IIS/MSIS Server - it should be selected by default
 - Click on **Services** - select the IIS Server - it should be selected by default
 - Click the **Stop** button 
 - Click the **OK** in the top right hand corner to close the IIS Server Service Manager

Restarting system services

The procedure uses the XML document from the **Services Server Configuration** in page 12.4.4.4.4

1. Stop the IIS/MSIS Server
The IIS/MSIS server may automatically start if it does not follow the procedure
 - In the Windows Task Bar -> double click the IIS Server icon 
 - Click on **Server** - select the IIS/MSIS Server - it should be selected by default
 - Click on **Services** - select the IIS Server - it should be selected by default
 - Click the **Stop** button 
 - Click the **OK** in the top right hand corner to close the IIS Server Service Manager
2. Stop the server hosting IIS/MSIS
Depending on the IIS/MSIS configuration the IIS/MSIS server may automatically start if it does not follow the procedure
 - In the user manager -> double click the IIS/MSIS user (see below) to start IIS/MSIS
 - Select the **Yes** next to **SetupServer.exe**
3. Stop the server hosting IIS/MSIS
Depending on the IIS/MSIS configuration the IIS/MSIS may automatically start if it does not follow the procedure
 - In the user manager -> double click the IIS/MSIS user (see below) to start IIS/MSIS
 - Select the **Yes** next to **SetupServer.exe**
4. Stop the IIS/MSIS Server
Depending on the IIS/MSIS configuration XML and the IIS/MSIS Server may automatically start if it does not follow the procedure

- In the Maintenance Task folder for Windows, select **Backup**.
 (This folder will appear as in the Custom Page or in the Properties folder of the Task name.)
- Right-click the server name and select **Run**.
- Click **OK**.

6. Start the server backup PDB.

Provided SQL Server Agent jobs

The following jobs are created and set up as scheduled by SQL utility.
 It supports only basic support.

SQL database

Task name	Description	Frequency
SQL server Maintenance Job	Backups and other user maintenance with no activity for more than a set determined number of hours. Default set is 12 hours.	Hourly
SQL server PDB, main Page	Page also updated based from the PDB table	Hourly

CRM database

Task name	Description	Frequency
SQL server Maintenance Job	Backups and other user maintenance with no activity for more than a set determined number of hours. Default set is 12 hours.	Hourly
SQL server, accounts, data, and report	Accounts separately selected report with no error (except for data) and then update accounts with no error and report	Hourly, midnight
SQL server, pending, data, and report	Page set of pending, that user accounts update a page in advance, then pending with error, with and with error report to error codes and	Hourly, 01:00:00

Worksheet name	Description	Frequency
100 - 1000 - 10000 100000 - 1000000	Trigonometric functions: sine, cosine, tangent, secant, cosecant, cotangent, and their inverses. Also includes the unit circle and arc length calculations.	Weekly, starting 100 - 1000

Function name	Description	Frequency
db_update_transactions_db	Recreates database upon transaction with its activity. It keeps the a pre-determined number of hours. Default set to 12 hours.	Daily
db_load_page_metadata update_db_stats i.e. db_load_page_block metadata	Load latest metadata to cache and if the corresponding data has been changed then the data.	Daily
db_update_db_stats update_db_stats	Updates the db_stats and the db_stats metadata.	Daily

Question no.	Description	Response
Q1. What is the definition of a group?	A group is a collection of individuals who are united by a common purpose or goal and who interact with each other to achieve that purpose.	Correct
Q2. What are the characteristics of a group?	The characteristics of a group are: (1) A common purpose or goal, (2) A collection of individuals, (3) Interaction between individuals, (4) A sense of unity or cohesion, (5) A set of norms or rules, (6) A system of roles, (7) A system of communication, (8) A system of decision-making, (9) A system of conflict resolution, (10) A system of reward and punishment.	Correct

Continuous job	Description	Frequency
Job name: Program, Maintenance	Performs routine maintenance on Workplace objects, such as objects in object spaces, object containers, etc. Though the intention is not to make errors, the job actually can unintentionally or purposely delete all of the work spaces. There is a two-second delay between iterations of processing of the work data.	Once per minute
Job name: DB, Purge, 100	Deletes the processing of work spaces used to update object demographic data with any changes. It also includes the processing of the Workplace work space, if applicable. Though the intention is not to make errors, the job actually can unintentionally or purposely delete all of the work spaces. There is a two-second delay between iterations of processing of the work space data.	Continuous

Continuous 100 db jobs

The job status reflects the result of the last execution of the job. The continuous jobs, the status may appear as Failed if the job was interrupted after being interrupted. If the job repeatedly fails, look in the job history, contact Pega Support.

Example: The 100, Server machine is scheduled after changing 100, Server Agent. Details changing and creating the job will reset the status.

Showing or Additional Jobs

If you the jobs listed above are not installed in your Workplace server, or you have additional jobs, contact your Pega implementation representative for confirmation as to the presence of these jobs.

Confirming installation of the Workplace server

- Go to the Workplace server: **Job Data - Programs - Microsoft SQL Server - 100, Server Management Studio**
- Click the job page next to your Workplace server.
- Click the job page next to the **Management** folder and then click **100**.
 The status of the job is displayed in the Status column.

Maintenance Jobs

Customer Required SQL Server Agent jobs

Customer Required SQL Server Agent Jobs

The following table contains the required database jobs that should be set up by your DBA when the database server is installed. These jobs are required for each individual database to help prevent application performance from degrading.

Note: Your DBA should set up replication jobs for the "MS" environment.

Below is a summary of the required maintenance jobs:

Database Job	Description	Recommended Frequency
IndexMaintenance	Analyze the table fragmentation in each database and defragment the database accordingly. For more information on table fragmentation, see Microsoft SQL.	Daily
Shrink-DB	Check for database overcommitment. For more information on table fragmentation, see Microsoft SQL.	Daily
Update statistics	Update the statistics that are used by the SQL Server query optimizer to choose the most efficient plan for retrieving or updating data. For more information on table fragmentation, see Microsoft SQL.	Daily

Note: These jobs should be set up by your DBA. If you do not have a DBA, then you can contact us to perform these tasks for you via our SQL Services program. Please contact us for more information.

Downloading Files From the Pica FTP Site

Requirements: In order to use the Pica FTP site, you must first obtain a user name and password from your Pica representative.

Downloading Files from the Free PDF site

1. It is a web browser, navigate to the website.
2. If it is the first time you have accessed the site, you will be prompted for a user ID and password.
3. Enter your User Name and Password, then click **Login**.
It enables viewing the folders on the PDF site again.
4. Double-click the **Folder** folder.
The folders within the **Folder** folder appear.
5. Double-click the **Download** folder.
The files and folders within the **Download** folder appear.
If you see the file you want, go on to the next step. If not, you may have to open some of the folders in the window to find the file.
6. Double-click the file you want.
The file download begins again.
7. Select **Save File To Disk**, then click **OK**.
The files are being downloaded.
8. Check the download status of the files in progress, under **Network Neighborhood**, then select your file, select.
9. Double-click your file, select. Then double-click your **Folder** folder, and then click **Save**.
It completes the operation on the file download.
10. Make sure the files download completely by visiting the file page on the PDF web site and then comparing it to the size of the file you downloaded into your **Folder** folder.
11. Send an email confirmation to your Print representative when all files are downloaded.

Maintenance Schedule

The following table gives you an example maintenance schedule for your Print Representative and critical field support. Tasks are suggested based on when they should occur.

- Weekly: Once per shift on the next day.
- Monthly: on the next day.
- Once a Day: on the next day.
- Once a Week: on page 10.
- Once a Month: on page 10.

Note: This is only an example. You may need to alter the schedule to your own requirements. See Maintenance Jobs on page 12 for detailed information on system maintenance.

[illegible]

Task	Points
Design the Database (20)	Design the database schema. Database will have approximately 10 tables. The relationships in database will be approximately equivalent to steps 10 to 14 of the 15 steps in Design a Database (20). The database is designed with 10 tables. Steps 10 to 14 of the 15 steps in Design a Database (20).

Type	Source
Change the Database URL	Change the default URL. Database URL: New connection, completed the configuration in Database URL, the connection is successful. At step 10 the status of the is Change a Database URL. New connection, completed the. Connect again, URL is step 10. We will it really. Database URL.

Task	Notes
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. A number of zone messages are stored in the MPT. Messages include alarm, warning, and message. Determine the current state of the equipment log for the zone and ensure that it is log for that is continuously. Verify that the current zone log for the
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.

Check & Work

Task	Notes
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.
Check the MPT (MPT) zone log	Check the MPT (MPT) zone log. Verify that it is other mode (e.g., log) or continuously.

Check & Work

Task	Notes
------	-------

Task	Notes
Check that the status of the connection is 'Connected'.	Check at step 11 of the setup wizard in the appropriate client application when the application is functioning in step 12 of the connection procedure. Any substantial decrease in the data speed should be investigated to determine the cause.
Review the connection and bandwidth management settings.	See How to Review Management Settings on page 12. See Set Up Data Speed .
Check the log file.	Log files for the Wi-Fi 6E™ technology are stored in folders by log date. Check the log file to find up status in the connection procedure. Note: If you have more than 1000 connecting volume more than 1000 messages are stored and may need to delete Wi-Fi 6E™ log files more often.

SQL Server Password Configuration

The Performance and Critical Task applications use a single SQL login when connecting to the database on the SQL Server instance. The login is defined with sufficient rights, allowing the application to connect, read, and update data in all of the system databases.

System administrators, in cases with the required rights, have the ability to change the SQL login password through the SQL Login or Users tab within the SQL Login or through a SQL tool is located on the server where the Performance Services are installed.

Below are the steps required to change the SQL Server login password, as well as technical details describing the functionality.

Note: Changing the password affects all system databases in all instances on the SQL Server. Performance and Critical Task applications do not need to be manually updated with the new password.

Note: The SQL login that is setup with system rights should be the only user accessing the SQL server.

Change the SQL Login password

In order to change the SQL login password, users must:

- Use a domain account.

SQL Server Password Configuration

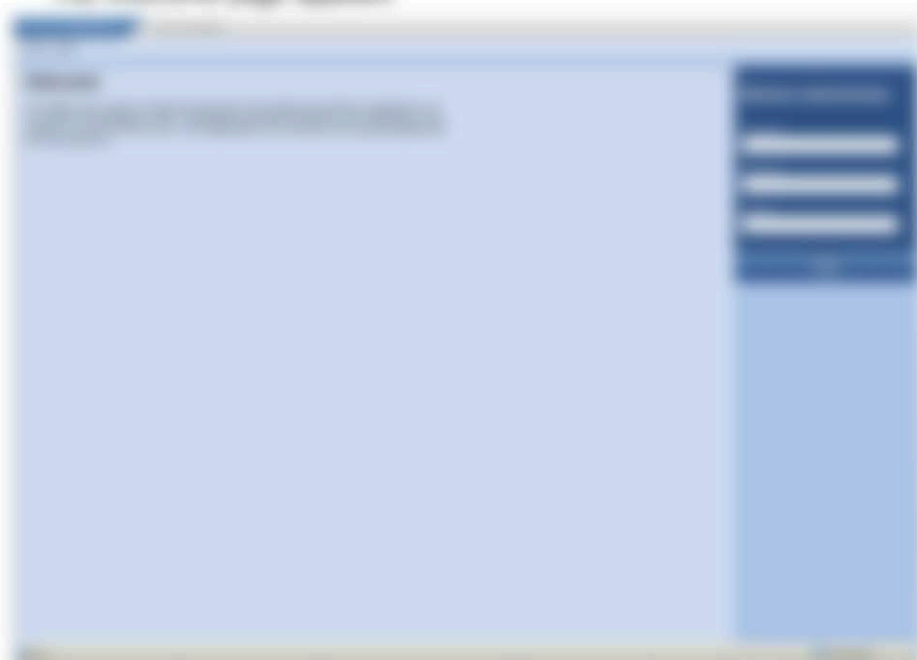
Change the SQL login password

- When system administrator rights in the SQL Services that will be affected by the password change are available, it can be performed on the SQL Server console. The user must have the appropriate rights in both SQL services.

Note: New passwords must be at least eight characters long and contain both a letter and a number.

Changing the SQL login password

1. Go to `http://ProvisionManagement/ugp/SQLConfiguration.aspx`
`ugp/SQLConfiguration.aspx` is the name of the page under Services console.
 The Services page appears.



2. Click the **Configure Password** and **Storage** of the user with rights to change the password in the corresponding fields and click **Save**.
 The Change SQL Password page appears.

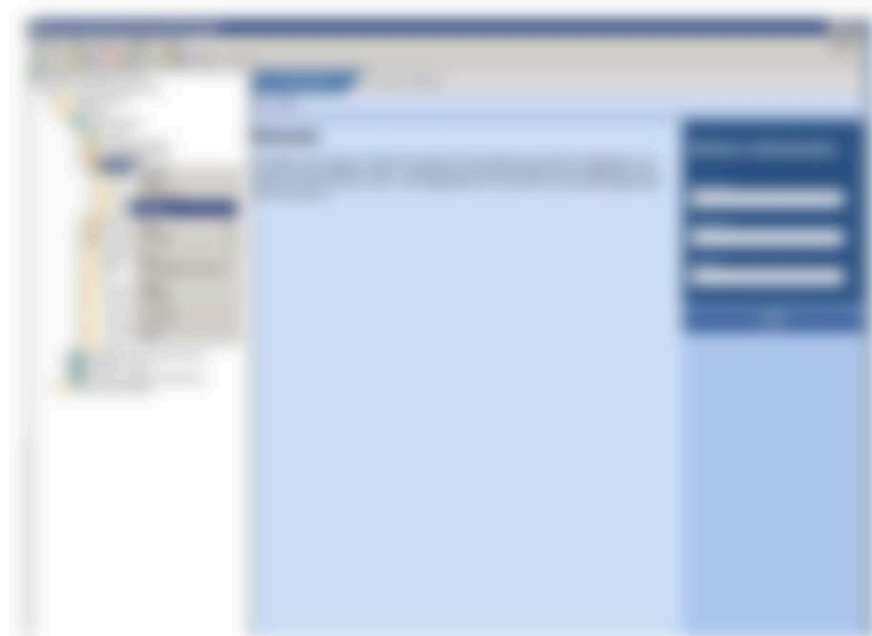


- c. Type the new password and then confirm the password is correct. See step 5b.
- d. Confirmation message should appear that the password has been changed successfully.
- e. Close the window.

Troubleshooting

As this is a website, all must be working to access the Web Server Password Configuration page. Check the network information Service Manager to ensure the folder "Logistics" exists.

To confirm your connection, right-click the folder and click **Browser**. The WebServer page should appear in the right pane, as shown below.



Reportuser SQL Trace

SQL Trace Overview

A single SQL user may have been created for use with Plus Performance and Critical Trace tools, and additional SQL users may be created for Performance and Critical Trace products, other to this release are no longer supported and will eventually be removed with the exception of reportuser. The reportuser user remains in place and will continue to be usable if the user needed at your site in a previous release, but it is no longer defined or supported.

The single SQL user is used to ensure compliance with security protocols. To capture multiple SQL users in a single SQL user, there may be a need to audit across the activity of these users in the SQL server. This section describes how to trace the activity of a SQL user.

In this chapter, **reportuser** is the SQL user being traced. To capture the activity of the reportuser, a server-side trace should be set up in the SQL Server to enable a trace file of the required activities listed below.

- Reportuser logins/logouts
- Objects used by reportuser
- Queries run by reportuser

After these activities have been gathered, the trace file can be viewed using SQL Profiler.

Appendix B: Trace

Trace SQL User Activity

Trace SQL User Activity

Tracing SQL user activity is a two-step process, with different methods for gathering user data. Review the options below and then choose the methods that best suit your needs.

Tracing user activity

1. Choose a trace method

Method A	Use the required information in the example script that has been provided and then set the script to perform the trace. To use this method, access the SQL Enterprise Manager SQL Server user activity trace information not available in the system settings. To add the example procedure, insert/replace the code for the following procedure:
Method B	Manually create a trace based on the required components. To manually create the trace, use the components table in section Chapter 13, Components of the Trace, page 13.

2. Choose how you want to start the trace

Method A	Manually start and stop the trace by running a script. For the required script information, see the topic Starting and stopping a user manually trace.
Method B	Configure the trace to start automatically when the SQL Server is started. For the required script information, see section Configuring the trace to start automatically when SQL Server starts in the Trace, page 13.

Starting and stopping a trace manually

- To manually start the trace, use the following script against the SQL Server instance that is, `servername`, in the procedure name:

```
USE master;
GO
EXEC sp_trace_initialize_with_args @start=1, @traceid=1, @maxfilesize=5000000, @on=1;
```

The command returns a traceid value, which is used to stop the trace.

- To stop the trace, use the following script against the SQL Server instance `servername` in the value of the trace:

```
USE master;
GO
EXEC sp_trace_setstatus @traceid=1, @status=0;
```


Appendix B: Table

Required Table Components

Appendix B: Specify the column to update

Column ID	The ID of the column you want to update
is	Whether you want to set the value to is or all

Note: For information, see the Microsoft article "SQL Server 2008: How to update data" <http://msdn.microsoft.com/en-us/library/ms188769.aspx>.

Appendix B: Filter the rows that is returned

Column ID	The ID of the table
Column ID	The ID of the column you want to set the filter on
operator	Specifies whether this is an AND or OR operation
value	Specifies whether the value is equal, greater than, less than, etc.
value	The value to use for your comparison

Note: For information, see the Microsoft article "SQL Server 2008: How to update data" <http://msdn.microsoft.com/en-us/library/ms188769.aspx>.

Appendix B: Specify the columns of the table

Table ID	The ID of the table
Column	Any, none, or column names

Note: For information, see the Microsoft article "SQL Server 2008: How to update data" <http://msdn.microsoft.com/en-us/library/ms188769.aspx>.

Peers Configuration Wizard

Peers Configuration Wizard Overview

The Peers Configuration Wizard is used to create or change the configuration of a machine that has virtual network components installed. To select the required components are installed in the following sections, respectively:

Step 1: 1. To prepare the configuration

Step 2: 2. To configure

Note: Information rights are required to use the Peers Configuration Wizard.

Note: The Peers Configuration Wizard must be executed from the machine that requires configuration.

One example of when you would need to update a configuration's configuration would be if the Configuration Service is moved. The configuration should be updated to point to the new location. Below is a summary of the configurations you can change using the Peers Configuration Wizard:

- Configuring a new configuration on the next page
- Configuring the VDI device on page 10

The Configuration Wizard is composed of two components that work together:

- ConfigWizard: the wizard where users input data
- ConfigTool: connects the wizard and the actions based on the parameters entered in the wizard

Free Configuration Wizard

Free Configuration Wizard Overview



There are two new files that are generated by the Configuration components, which are useful after configuration:

- Configuration log: A log file is generated with any errors which you view the Free button in the Configuration.
- Configuration file: The file generated by the Configuration component has utility, which is useful after the user click the Free button in the Configuration. Reference the file to make other settings the configuration changes.

Configuring a New Workstation

1. Welcome to the "Free Configuration Wizard" window and double-click Configuration Wizard to open the Free Configuration Wizard.
2. Select **New Workstation** and click **Next**.
The Free Configuration Wizard opens.
3. Enter the name of the Free Configuration Wizard and click **Next**.

Note: If the name of the Flow, such as Service, is changed, the ConfigWizard must be executed in the code, and Flow is added to the log. The Flow, such as Service, cannot appear with the new name name. (Note: Flow is not used.)

The Department, Faculty, and Location window appears.

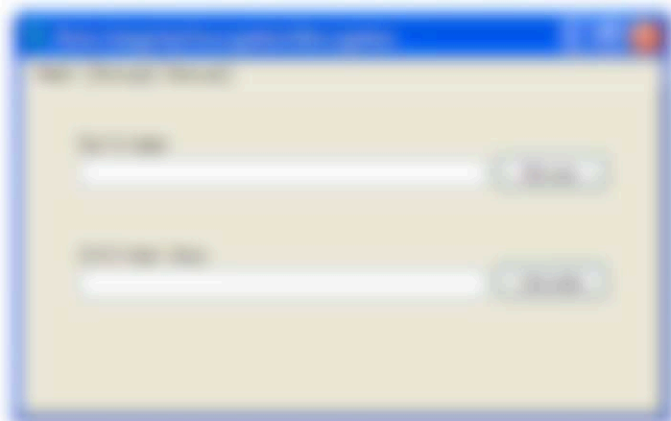
1. Specify the Department, Location, Website, and Description Type.
To add a new Department, select "I want to add a new Department" and enter the required details in the available fields.
2. Click **Next**.
The Summary window appears. Review the Configuration Summary to make sure the settings are accurate.
3. Click **Finish**.
A confirmation window appears.
4. Click **Yes** to proceed with your selection of a new configuration. (Note: **No** is not an option.)
Click **Yes** to return to the Summary window and edit the settings.

Configuring the FIM Server

1. At the FIM screen, click the FIM Wizard and launch Flow Service services.
2. Browse to the "FlowConfiguration" folder and double-click ConfigWizard.exe to launch the Flow Configuration Wizard.
3. Select **FIM Server** and click **Next**.
The Flow, such as Service, window appears.
4. Enter the name of the Flow, such as Service, and click **Next**.
The Summary window appears. Review the Configuration Summary to make sure the settings are accurate.
5. Click **Finish**.
A confirmation window appears.
6. Click **Yes** to proceed with your selection of a new configuration. (Note: **No** is not an option.)
Click **Yes** to return to the Summary window and edit the settings.
7. Review the FIM Wizard and launch Flow Service services.

File Integrity/Encryption/Decryption Tool Overview

The File Integrity/Encryption/Decryption tool (Crypto Tool) allows users to generate hash values, and encrypt/decrypt files that are generated by the FileSignature and FileIntegrity tools applications to ensure their confidentiality and protect their contents. This tool is mainly intended for use with files that will be used in an encrypted system, but can also be used to protect files in plaintext when they



- **Hash generation** is unique values for a file to ensure that its integrity has not been compromised. Once a hash value is generated, you should store it separately in a suitable location for reference.
- **Encrypt** secures a file to protect its contents.
- **Decrypt** secures a file so only users with the required password can access its contents.

Crypto Test

Access the Crypto Test

Note: This test must be accessed from a workstation that meets the software requirements, which are available in the Release Notes.

Access the Crypto Test

The Crypto Test of PowerCrypter.com is available upon request.

Hash, Encrypt, or Decrypt a File

Hashing, encrypting, or decrypting is the regular process in the Crypto Test. See Access the Crypto Test section for details on accessing the test.

Hashing a File Value

1. Open the Crypto Test either by double-clicking the file PowerCrypter.exe or from a menu within the application.
The Crypto Test appears.
2. Click the **Hash** tab.
3. Click the **Browse** button and find the file you want to hash.
4. Select the file and click **Open**.
The path appears in the File To Hash field.
5. Click the **Calculate** button to calculate a hash value for the file.
6. Save a copy of the hash value in a text document using Notepad or some other wordprocessing application to retain the value.
Note: In the second hash value when creating the file's integrity at a later time.

Encrypting a File

1. Open the Crypto Test either by double-clicking the file PowerCrypter.exe or from a menu within the application.
The Crypto Test appears.
2. Click the **Encrypt** tab.
3. Click the **Browse** button and find the file you want to encrypt.
4. Select the file and click **Open**.

The path appears in the File to Storage using HTTP tool. By default, the corrupted file is saved in the same location where the original file exists with the suffix " corrupt". To change the corrupted file's destination, click the **Change** button and specify a new path.

1. Tap a statement for the corrupted file, and then change the statement to confirm its accuracy.

Note: The statement is required to corrupt the file.

2. Click **Storage**.

A message appears, confirming the successful corruption.

Corrupting a File

1. Open the Crash Test editor by double-clicking the file. The Crash Test editor is then opened within the application.

The Crash Test appears.

2. Click the **Storage** tab.
3. Click the **Change** button and then the file you want to corrupt.
4. Select the file and click **Open**.

The path appears in the File to Storage using HTTP tool. By default, the corrupted file is saved in the same location where the original file exists. To change the corrupted file's destination, click the **Change** button and specify a new path.

5. Tap the statement that was created when the file was corrupted, and then change the statement to confirm its accuracy.
 6. Click **Storage**.
- A message appears, confirming the successful corruption.

Meditech Extracts

Meditech Extracts Overview

For users integrated with a Meditech® EHR system, Meditech extracts pull data from that system into the Meditech database in the way outlined.

Meditech Modules

Data may be pulled from the following Meditech modules:

- A/R
- Admissions
- Medical Records
- Billing/Accounts Receivable
- Patient Management
- Scheduling
- Lab
- Imaging

Each Meditech module requires its own set of extracts.

Flags and Village Extracts

Extracts operate in both Flags and Meditech's proprietary Village client server platforms.

Extracts in Flags platforms have two parts:

- **Connected** means that the external programs are actively exchanging data.
- **Collecting** means that the external programs are waiting for data. That is, they have processed all of the available data and are waiting for more.

Turning off Redshift Stage Jobs

1. From the **UI** menu, click **Stage Jobs** under the **UI** Redshift Stage Jobs menu item.
2. From the **Stage Jobs** page, toggle the **Stage Jobs** switch to **Off**.
3. It may take a few minutes for all the jobs to stop. You may need to wait 15 minutes to refresh the display.

Turning off Redshift Workflows

1. From the **UI** menu, click **Workflows** under the **UI** Redshift Workflows menu item.
2. From the **Workflows** page, toggle the **Workflows** switch to **Off**.
3. The workflows will stop their run at a time. To resume the process, click **Turn On** under the **Workflows** menu item.

Tallman Medication Update Overview

The Tallman Medication update will change medication description data to match the data approved by the FDA and NDA. An example of an update would be changing the description from "anticoagulant or thrombolytic" to "anticoagulant or antiplatelet". The data that changes in the Tallman update are FDA and NDA medication data updated using source provided by First.

MDL Database

The script to update the MDL database will update the Medication and the Treatment database table. In the Medication table the MedicationName column is updated to match Tallman data. In the Treatment table the MedicationName column is updated to match Tallman data.

Note: The script may generate a message indicating that it cannot be run because of duplicate descriptions. These are cases where there have been changes to the Medication database table. If duplicates are found they will need to be resolved before the script is run.

CDL Database

The script to update the CDL database will update the Drug database table. In the Drug table the MDLName column is updated to match Tallman data.

Running the Tallman Medication Update

1. Browse to the folder: `\\first-cblm01\first\bin\update\updateMDL`
2. Run the MDL Tallman medication update script: `updateMedicationDescriptionsToTallman.cmd`

Tablet Medication Update Exercise

Review the Tablet Medication Update

1. Review the table "New Monthly Prescriptions/Refills (NPR)"
2. Run the 2019 Tablet Medication Update script. Update Medication Descriptions in Tablet Data set

Technical Notes

Technical Notes Overview

This chapter includes technical information that may be pertinent to users, depending on their system components.

File Save Restrictions

Some Perspectives and Outlook data programs include functionality for saving files. Users may find that it is not possible to save the file in certain file formats, such as the "PageMaker" file. This is due to the Windows 7 operating system feature called file format restrictions, which is enabled by default. Users can disable such file restrictions, subject to their own security policy. It is not intended, nor is desired, that it should make users aware of the restrictions. For more information, see [MSDN](#).

For more information, see [http://msdn.microsoft.com/Windows7/itpro/itpro.mspx](#).

Note: This file save restriction only applies to users using Windows 7.

External Report Scheduler

The External Report Scheduler uses all the report options as if it is a report-schedule location. The Print Report Service (PRS) generates the reports and runs on the administrative server where Print Audit Services are installed. There must be connectivity between the report-schedule location and the administrative server in order for the report to be reported.