Technical Reference Guide

Picis Perioperative and Critical Care 10.0C

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 *Release Notes*.

Contents

Contents

1 Introduction

About this Guide

This guide is intended for system administrators at hospitals and Picis partners with responsibility for technical aspects of a Picis Perioperative and Critical Care installation. Readers should have technical knowledge and experience with installation and configuration of client/server systems. The focus of this guide is on the latest version of Picis Perioperative and Critical Care, although some topics are also applicable to previous versions.

The guide should be used in conjunction with the following documents:

- Installation Guides
- System Configuration Guide
- Workstation User Guide
- PCM Documentation

Terms and Concepts

Expression	Definition
“Administrative modules” system	A networked system of servers and workstations running OR Manager. (It may also include OR Manager Web Access and/or SmarTrack). Some workstations will also run Security Manager, the tool used to control user and group access to modules. The basic “administrative modules” system uses three databases (PSM, ORM and IDB.) If SmarTrack is installed then yet another database is needed (TRK).
ADT	Admit, Discharge, Transfer.
Browser-based (thin) clients	OR Manager Web Access and/or SmarTrack Thin Client and/or Perioperative Analytics.
CAR	"Clinical modules" database
“Clinical modules” system	A networks system of servers and workstations running one or more of the following modules: Preop Manager, Anesthesia Manager, PACU Manager Critical Care Manager. The system uses the CAR and PSM databases.
Clinical services	Includes services used by the “clinical modules,” (PCM, Printouts Service).
Content Library	Contains a comprehensive set of documentation methods from which clients can select the category of content they would like to install. The Content Library is also used for the incremental delivery of new content geared towards best documentation practices. This content is installed using the Content Library installer.
Data Load	The creation and filling of “administrative module” databases with “static” hospital content. This is usually performed in house prior to shipping the database(s) to the client site for installation.
IDB	Interface database
MM	Materials Management

Expression	Definition
Move Live	After creating a TEST database for the first time, the move-live process is used to duplicate that database for use in a LIVE environment. (The process is not relevant for databases that are being upgraded).
ORM	OR Manager database
PSM	Security Manager database
PRS	Pics Report Scheduler
Public folder	The term "Public folder" refers to the shared folder location where the Peroperative and Critical Care software installation resides. The exact name of this folder may vary, but the location where the installed software exists is referred to as the Public folder throughout this document.
“Test”, “Live” and “Dev” environments	In addition to TEST and LIVE environments, sites that are already LIVE with one product and want to install additional modules to become a TPA system will need a third environment-DEV. The DEV environment is used for building the integrated TPA system while leaving the TEST environment free for troubleshooting and testing any service packs or minor updates that may be required during the time it takes to implement the TPA system. (The DEV environment is only supported until the TPA system goes LIVE. Then the DEV environment becomes the new TEST environment and the existing TEST environment is annulled).
Total Perioperative Automation (TPA) systems (also known as Perioperative Integration)	Integration between a “clinical module” system and an “administrative module” system such that certain patient data is shared between them. Also called “integrated systems”. (Unless otherwise specified, the terms integrated and integration refer to perioperative integration).
Transaction processor	“Administrative module” components that carry out specific tasks related to the data flow within an administrative system (Surgsync, Autoprint, CareTaker, HL7 Interfaces).
TRK	SmarTrack database

2

Technical Overview

Standard Server Configuration

Picis Perioperative and Critical Care is a client/server system that uses multiple databases (housed on one server) and a number of background servers (depending on your system).

A standard “TPA” server configuration is made up of a server where the application databases are stored, a separate server where “clinical modules” components are stored (typically referred to as the “clinical modules” server), and another server where the “administrative modules” components are stored (typically referred to as the “administrative modules” server).

Below is an example of a standard “TPA” server configuration. Most sites will follow this server configuration, even if some of the installed components vary.

Note: For Non-VA sites, "clinical module” systems can be integrated with a third-party ORMS system. In this arrangement, SmarTrack is accessible from Anesthesia Manager and the system can be linked to the hospital billing system. (OR Manager is still used for configuration and behind-the-scenes data flow but end users do not interact with it. The system components and configuration are basically the same as for a "TPA" installation. For this reason, sites wishing to implement such a system should follow the “TPA” instructions found within this guide.

For VA sites, "clinical module” systems can also be integrated with SmarTrack but in this case OR Manager is not used at all. The system components and configuration are the same as for a "standalone clinical module" installation with the addition of the TRK database and VA-specific suitekey..

Note: Picis Perioperative Analytics is an optional feature and requires additional servers to accommodate functionality. The installation of these features is described in their respective installation guides.

Standard “TPA” System

Machine	Hosted Components
Database server	Live databases Test databases \\Public share
Analytics server	Business Objects, Extelligence OR/Anesthesia, Perioperative Dashboard
Live “administrative module” server	Picis (web) Services Autoprint, Content Library Installer, CareTaker, Meditech Extracts, PMR, Analytics Control Portal, Surgsync, OR Manager Web Access, SmarTrack Web Access
Live “clinical module” server	Data Sync, PCM, Customize, eView, Clinical Notes System
Test “admin” and “clinical” module server [a]	Picis (web) Services Autoprint, Content Library Installer, CareTaker, Data Sync, Meditech Extracts, Picis Connectivity Manager, PMR, Analytics Control Portal, Surgsync, OR Manager Web Access, SmarTrack Web Access, Customize, eView, Clinical Notes System
Live Desktop PC	DB Utility, OR Manager, SmarTrack, Security Manager, DB Editor, Customize, Preop Manager, and Anesthesia Manager[b] (Minimum machine specification is that of a workstation)
Test Desktop PC	DB Utility, OR Manager, SmarTrack, Security Manager, DB Editor, Customize, Preop Manager, and Anesthesia Manager[b] (Minimum machine specification is that of a workstation)

a. In the Test environment, the “administrative module” and “clinical module” server components are combined.

b. PACU Manager or Critical Care Manager might be installed instead of Anesthesia Manager.

Standalone “Clinical module” System

Machine	Hosted Components
Database Server	Live databases Test databases \\Public share
Analytics server	Business Objects, Extelligence OR/Anesthesia , Perioperative Dashboard
Live “clinical module” server	Content Library Installer, Picis Connectivity Manager, Analytics Control Portal, Customize, Picis (web) Services, eView, Clinical Notes System
Test “clinical module” server	Content Library Installer, , Picis Connectivity Manager, Analytics Control Portal, Customize, Picis (web) Services, eView, Clinical Notes System
Live Desktop PC	Anesthesia Manager[a], DB Utility, DB Editor, Customize (Minimum machine specification is that of a workstation)
Test Desktop PC	Anesthesia Manager[a], DB Utility, DB Editor, Customize (Minimum machine specification is that of a workstation)

[a] *PACU Manager or Critical Care Manager might be installed instead of Anesthesia Manager.*

Standalone “Administrative module” System

Machine	Hosted Components
Database Server	Live databases Test databases \\Public share
Analytics server	Business Objects, OR/Anesthesia Extelligence, Perioperative Dashboard
Live “administrative module” server	Autoprint, Content Library Installer, CareTaker, DB Utility, Meditech Extracts, Picis Message Router, Analytics Control Portal, Surgsync, OR Manager/SmarTrack Web Access, Picis (web) Services
Test “administrative module” server	Autoprint, Content Library Installer, CareTaker, DB Utility, Meditech Extracts, Picis Message Router, Analytics Control Portal, Surgsync, OR Manager/SmarTrack Web Access, Picis (web) Services
Live & Test Desktop PC	OR Manager, SmarTrack, Security Manager (Minimum machine specification is that of a workstation)

Notes:

- Your exact configuration depends on the modules you are installing. For example, if you are installing OR Manager and Anesthesia Manager in an integrated system, you are likely to have a configuration similar to the standard “TPA” server configuration above. However, if you are installing just OR Manager or just Anesthesia Manager, you will have a server configuration that is designed for that type of system.
- All machines should meet the minimum hardware specifications outlined in your site’s contact. For more information, please consult your Picis representative.
- For information regarding a file save restriction associated with Windows 7 operating systems, see *Technical Notes* on page 153.

Standard Server Components

Below is a description of the background server components.

- **Database Server**: A standalone server (or servers) for the application databases, where TEST and LIVE database environments are installed. A shared folder named “Public” is also created where the installation files for all software are stored.
- **Picis Message Router** (PMR): This service manages integration with other hospital systems such as the Hospital Information System or Materials Management System for OR Manager. (For more information, see *PMR Service* on page 30).
- **Surgsync:** This executable checks updates to patient-related data sent from external systems and transfers this data to the OR Manager database. (For more information, see *Surgsync* on page 32).
- **Autoprint**: This executable publishes changes to scheduling data in OR Manager to specified recipients via printout or email. (For more information, see *Autoprint* on page 38).
- **Picis (web) Services**: The catalog of centralized, back-end web services that supply capabilities and data to applications and other Picis Perioperative and Critical Care components. (For more information, see *Picis (web) Services* on page 24).
- **Printouts Service**: This service controls automatic silent printing for Anesthesia Manager.
- **Picis Connectivity Manager** (PCM.NET): This service manages integration with other hospital systems such as the Laboratory Information System or Order Entry System. It is also responsible for the bi-directional flow of information between Perioperative and Critical Care modules. (For more information, see *PCM Service* on page 26).
- **Customize**: Customize is used to control server and workstation configuration settings. For more information, see the *System Configuration Guide*.
- **Application Test Workstations:** A version of the application software will be installed to allow off-line testing and troubleshooting.

Standard System Databases

A Picis Perioperative and Critical Care system requires a dedicated database server. This contains multiple databases to support the corresponding module(s). Each module requires a different database as described in the following table.

Application Name	Database Name	Purpose
OR Manager	ORM	Contains booking and case record information for a patient.
Security Manager	PSM	Contains user access rights and group security information.
N/A	IDB	Temporary repository for all information sent to or from external systems.
SmarTrack	TRK	Extracts and holds all information related to patient status for display on the SmarTrack screens.
Preop Manager Anesthesia Manager PACU Manager Critical Care Manager	CAR	Contains all information related to patients admitted to the “clinical modules”.

Note: The actual name of your databases may slightly differ; non-production databases are prefixed by the environment name. For example, *TestORManager* or *DevORManager*.

System Backup and Recovery

Picis 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. (For more information about backups *Database Backups* on page 115). The “Public” folder should also be backed as it is the master source of Perioperative and Critical Care software for the site and where any new configuration files are stored.
- **Surgsync**: No data is stored on the Surgsync background server so it is not necessary to backup anything where it resides.
- **Autoprint**: No data is stored on the Autoprint background server, so it is not necessary to backup anything where it resides.
- **PMR Interface files:** PMR Interfaces include configuration and translation files that should be backed up regularly to preserve settings. These files exist in the Interface installation folder (typically “C:\Picis PMR\<PMR Interface folder>\Settings” and “C:\Picis PMR\<PMR Interface folder>\Translations).”

- **Clinical Services** (PCM and the Printouts service): If a service is not available the message will be resent. Configuration information is stored in the CAR database, and the settings are configured via Customize.

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

- *Picis (web) Services* on page 24
- *PCM Service* on page 26
- *PMR Service* on page 30
- *Printout Service* on page 32
- *Picis Report Service* on page 32

BACKGROUND APPLICATIONS

- *Surgsync* on page 32
- *Autoprint* on page 38
- *CareTaker* on page 43

Picis web services are installed using a dedicated installer. The other services and applications are installed using the Server installer. (The Suitekey combination determines the actual components installed. For more information, see the *Picis Internal Information Document*.)

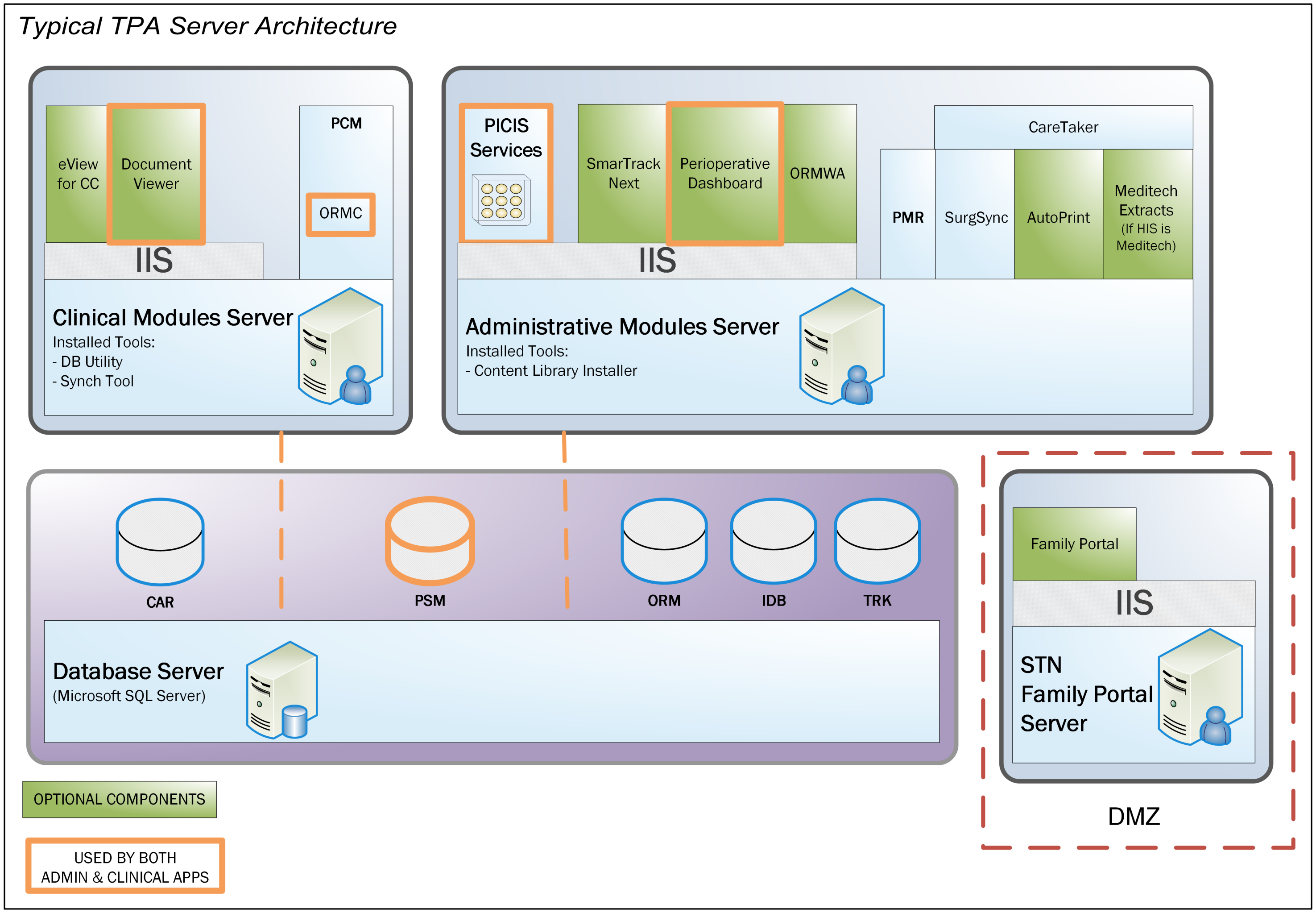
The following diagram shows a typical TPA server system.

Server Architecture

This section includes the following diagrams:

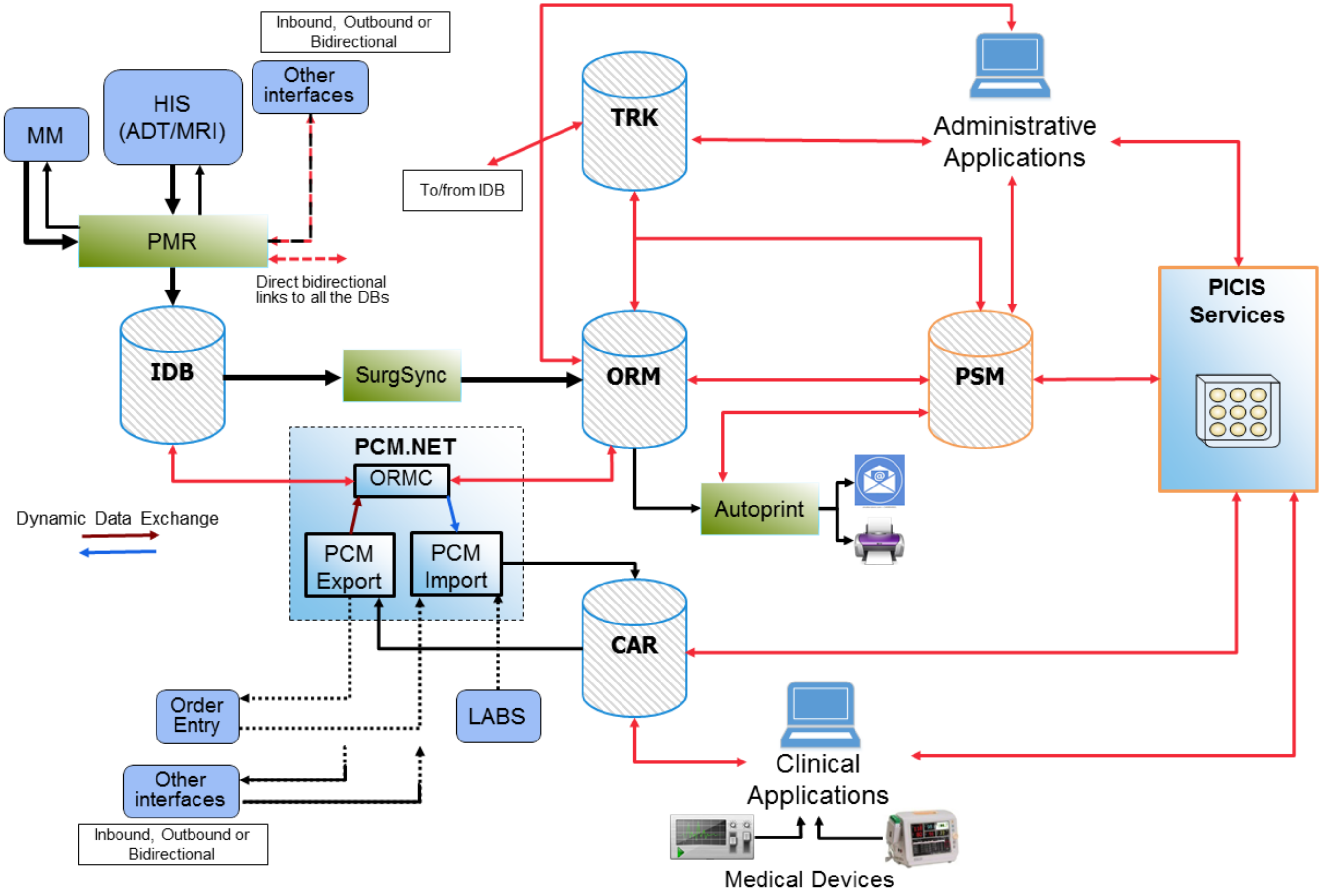
- Typical TPA server architecture
- Typical TPA server data flow

Note: For a standalone "clinical module" system, Picis services, the Perioperative dashboard and the Content Library installer are installed on the "clinical modules" server.


Typical TPA Server Architecture
eView for CC
Document Viewer
PCM
ORMC
IIS
Clinical Modules Server
Installed Tools:
- DB Utility
- Synch Tool
PICIS Services
SmarTrack Next
Perioperative Dashboard
ORMWA
CareTaker
PMR
SurgSync
AutoPrint
Meditech Extracts (If HIS is Meditech)
IIS
Administrative Modules Server
Installed Tools:
- Content Library Installer
CAR
PSM
ORM
IDB
TRK
Database Server
(Microsoft SQL Server)
Family Portal
IIS
STN Family Portal Server
DMZ
OPTIONAL COMPONENTS
USED BY BOTH ADMIN & CLINICAL APPS

Typical TPA Server Data Flow

Bidirectional flow in red
Inbound HIS and MM data flow shown with large arrows



Picis (web) Services

Picis (web) Services are the first components required to be installed for Picis Perioperative and Critical Care. The installer deploys the web services and web applications required for the server components and desktop applications, in order to facilitate database connectivity and other configuration settings. Each service has a *web.config* file where configuration settings are stored.

The Picis (web) Services are installed on one background server, which is determined depending on the system ("TPA" or "non-TPA"). Once installed, each Picis Service has a virtual directory in IIS and runs in its own application pool in IIS based on its name. The Picis (web) Services are configured in IIS to automatically start on reboot or restart to provide better performance to the calling applications.

Clients of the Picis (web) Services (applications) use Windows Communication Foundation's TCP/IP protocol to communicate with the services rather than http protocol. This configuration is described as part of the installation steps (see the *Server Installation Guide* for port information).

Each service includes logging capabilities to trace errors and other messages. For information on logging, see *Picis (web) Services Diagnostics* on page 64.

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

Note: For Picis (web) Services installation and troubleshooting information, see the *Server Installation Guide* appendix.

List of Picis services:

- ADT Service
- Configuration Service
- ClinicalPatientData Service
- Demographics Service
- Orders Service
- Patient Information Service
- Preop Service
- Security Service

ADT Service

The ADT Service facilitates the main ADT workflows, including the following ADT system operations:

- Pre-admit a patient
- Admit a patient
- Discharge a patient
- Transfer a patient
- Book a patient
- Update an existing booking
- Cancel an existing booking
- Undo a previous discharge
- Check if transferred patients should be automatically discharged

Configuration Service

This service allows all of the applications and other Picis services to connect to the databases by retrieving the database connection strings and the associated database credentials. All of the other Picis services and web applications access the Configuration service.

In addition to enabling database connections, the Configuration service stores the database login user name and password credentials in a standalone XML file; these credentials must match what is in the actual database. The Configuration service also provides the ability to read and modify configuration values for "clinical module" applications, which are stored in the database.

ClinicalPatientData Service

For systems that include "clinical modules" the ClinicalPatientData Service service provides data to the Patient Summary for Labs, VitalSigns, events, and the Clinical Notes System.

Demographics Service

This service creates, retrieves, and updates patient demographic information between the workstations and the CAR database.

This service also provides an interface to implement the Integrated Fields feature.

Orders Service

For systems that include "clinical modules" the Orders service provides data to the Patient Summary for Fluid Balance, Scores, Assessments, and Medication Orders. The Orders Service is also used to implement the following functionality:

- Forms Builder: Fluids in/out component, Fluid action details component, Medications component, Medication details component, Nursing Care component

- Protocol improvements/Move Order
- Discontinue orders for the Auto Discharge
- Scores enhancements
- Clinical Notes System

Patient Information Service

The Patient Information Service enables an updated method for retrieving Patient Summary Report data for the eView, Anesthesia Manager, Critical Care Manager, PACU Manager, and OR Manager applications. This service relies on other services (Demographics, ClinicalPatientData, Orders, and Preop) to retrieve the corresponding patient summary information. The PatientInformation Service also provides an interface to implement the Required Fields feature.

The Anesthesia Manager/Critical Care Manager/PACU Manager applications use the .NET TCP/IP binding to communicate with the Patient Information Service, and the Patient Information Service uses .NET pipe bindings to communicate with the local Clinical Patient Data, Orders, and Preop Services.

Preop Service

For systems that include "clinical modules" the Preop Service provides data to the Patient Summary for allergies, diagnoses, and procedures.

Security Service

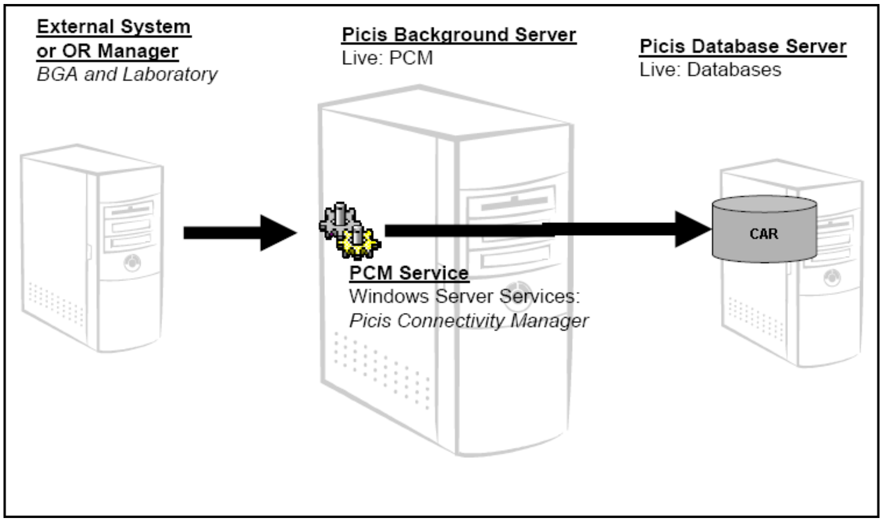
This service provides a single point of entry for authentication, authorization, password change functionality, and login auditing functionality for Analytics Control Portal, eView, and the “clinical modules” applications and server components.

Web Applications

In addition to the individual services that are installed, the Picis (web) Services installer includes the web application that enable access to the SQL login password configuration (LoginSqlUI).

PCM Service

Picis Connectivity Manager (PCM.NET) is a Windows service that runs on a background server and processes messages received from external systems. PCM.NET Service also processes the bidirectional flow of information between OR Manager and Preop Manager, Anesthesia Manager, PACU Manager, or Critical Care Manager.



PCM.NET Service Maintenance

The PCM.NET Service maintenance consists of ensuring the PCM.NET Service and PCM.NET Service clients are running and that there is an available connection to the external systems.

A message logging tool is available to log outbound message statuses as they are sent via PCM.NET. This tool must be enabled for use. For more information on the HL7 Outbound Message Logging tool, see the *Activity Logs & Diagnostic Tools* on page 53.

Managing the PCM.NET Service

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

1. Click **Start** > **Administrative Tools** > **Services** to open the Services console.
2. Right-click **Picis PCM.NET 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 start the service.
3. Click **OK** to close the Properties window.

Configuring the PCM.NET 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 **Picis PCM.NET Service** and select **Properties**.
3. From the drop-down menu next to **Startup type**, select **Automatic**, **Manual**, or **Disabled**.
4. Click **OK** to close the Properties window.

PCM.NET Service Troubleshooting

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

- *Updates not sent to application* below
- *Missing data elements* below
- *Checking the PCM.NET Service messages folders* on the facing page
- *Processing batch PCM messages* on the facing page
- *Viewing the “PCM Rejected” table* on the facing page
- *Reporting a PCM.NET Service problem to Picis Support* on page 30

Updates not sent to application

Updates from external systems (HIS, LIS, etc.) are not seen in Anesthesia Manager, PACU Manager or Critical Care Manager.

1. Check the Picis PCM.NET Service. (See *Managing the PCM.NET Service* on the previous page for further information).
2. Check the intermediate folders (messages and old messages) for PCM.NET Service and PCM.NET Service client messages. (See *Checking the PCM.NET Service messages folders* on the facing page).
3. Use Perfect Trace to verify that messages are being received (and if not identify what is happening). (See *Perfect Trace* on page 56 for further details).
4. If the PCM.NET Service) appears unresponsive, then process batches of message files. (See *Processing batch PCM messages* on the facing page for further information).
5. Contact Picis Support. (See *Reporting a PCM.NET Service problem to Picis Support* on page 30 for further information).

Missing data elements

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

1. Check the PCM_Rejected Table. (See *Viewing the “PCM Rejected” table* on the facing page for further details).
2. Use Perfect Trace to verify that messages are being received (and if not identify what is happening). (See *Perfect Trace* on page 56 for further details).

3. Contact Picis Support. (See *Reporting a PCM.NET Service problem to Picis Support* on the next page for further information).

Checking the PCM.NET Service messages folders

Note: Messages sent in PCM synchronous mode will not leave messages. Synchronous messaging can be activated from the HL7 message or in the PCM configuration files. See PCM documentation from the *Picis User Community* at *https://users.picis.com* further information.

Note: This procedure is for the HL7 folders. If you are using another client, navigate to the equivalent folder locations for them and check that the messages are moved from the “messages” folder to the “old messages” folder.

- Navigate to the folder “C:\Picis\PCM\pcmImport\pcmImport\HL7\messages.” If there are any messages in this folder it will be because PCM cannot process them.

  Processed messages are moved to: “C:\Picis\PCM\pcmImport\pcmImport\HL7\oldmessages.”

Processing batch PCM messages

The procedure shows how to send batches of messages to the PCM. This procedure could also be adapted for any PCM client.

1. Stop the PCM.NET Service. (See *Managing the PCM.NET Service* on page 27 for further information).
2. In the “C:\Picis\PCM\pcmImport\pcmImport\HL7\” folder, rename the folder “messages” to “messagetmp.”
3. In the “C:\Picis\PCM\pcmImport\pcmImport\HL7\” folder, create a new folder called “messages.”
4. Copy messages from the “messagetmp” folder to the “messages” folder.
5. Start the PCM.NET Service. (See *Managing the PCM.NET Service* on page 27 for further information).
6. Verify that the messages have processed.

Note: You are advised to test this with a few messages at a time: in the first instance only copy a few messages to the “messages” folder in step 4.

Viewing the “PCM Rejected” table

The PCM_Rejected table holds copies of all messages rejected by the PCM and gives the reason for the rejection.

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

4. From the drop-down list, select the CAR database (the actual name may vary; for example, it could be liveaManager etc.).
5. Locate the message and review the PCM_Reason column.

Reporting a PCM.NET Service problem to Picis Support

If you are experiencing problems with PCM.NET Service and need to open a Service Request with Picis Support, please include the following information:

- A detailed description of the problem, including any screen shots if appropriate.
- A Perfect Trace log from the PCM.NET Service for a time period when the problem occurred. (See *Perfect Trace* on page 56 for further details).
- From the Advanced Configuration Editor in Customize, export the configuration settings under PCM and send them to Picis support.

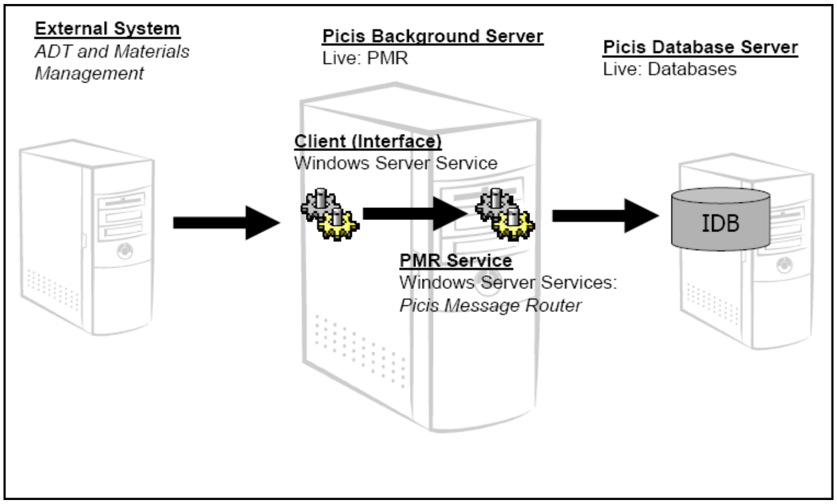
Further Information

For further information about PCM.NET Service installation, configuration, troubleshooting and development see the PCM.NET Service and interface documentation from the *User Community* at *https://users.picis.com.*

PMR Service

Picis Message Router (PMR) is a Windows service that runs on one background server and processes messages received from an external system.

The service is used by standalone "administrative module" systems and "TPA" systems.



PMR Maintenance

PMR maintenance consists of ensuring the PMR server service is running and that there is an available connection to the external system(s).

Starting, stopping, restarting, or viewing the PMR service

During normal maintenance, or as part of troubleshooting, you may be required to Start, Stop, Restart, or View a Picis service.

1. Click **Start** > **Administrative Tools** > **Services** to open the Services console.
2. Right-click **Picis Message Router** 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 start the service.
3. Click **OK** to close the Properties window.

Configuring the PMR 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 **Picis Message Router** and select **Properties**.
3. From the drop-down menu next to **Startup type:** select **Automatic**, **Manual**, or **Disabled**.
4. Click **OK** to close the Properties window.

Printout Service

The Printout Service is used by "clinical module" applications. Its purpose is to generate automated ("silent") printouts at scheduled times or in response to configured milestone events. The service behaves as follows:

1. The MILESTONES table is populated with a copy of the following events when they are documented for a patient case:
   - AdtTransfer (DBOID 066000000000018000000)
   - AdtDischarge (DBOID 066000000000019000000)
   - AutoDischarge (DBOID 66000000000085000000)
   - EditCloseDischargedRecord (DBOID 66000000000096000000)
   - EditClosePreopRecord (DBOID 66000000000097000000)
   - ALL MILESTONE Events with an EventType DBOID of 61000000000007000000
   - Events from the PCS_EVENTDATA table related to admitted patients (this table stores internal system events, such as "Patient record accessed".)
2. The service polls new rows in the MILESTONES table.
3. If a new event is configured to trigger a printout, or if a printout is scheduled for the current time, the service adds a corresponding row to the PRINTOUTS table.
4. The service processes new entries in the PRINTOUTS table and generates printouts according to the instructions in the PRINTOUTINFO column.

Picis Report Service

For systems that include OR Manager, the Picis Report Service (PRS) is used to generate external reports scheduled through the Report Scheduler. This timer-based service repeats the same task at regular intervals. The task determines which scheduled reports need to be run. The service will then spawn a process for each of those reports which will create the report in a shared folder, deliver as an email attachment, or both depending on configuration.

Surgsync

Surgsync is an application that resides and operates on the “administrative modules” server. (It is typically hosted on separate servers for TEST and LIVE environments.)

Surgsync performs the following tasks:

- Updates existing patient demographic data based on Admit, Discharge, Transfer (ADT) transactions.
- Updates and adds Materials Management (MM) stock items from an external MM system.
- Processes billing and MM reject files.
- Merges patient medical record numbers in OR Manager.

Patient Updates

When using an ADT interface, Surgsync updates patient demographics in OR Manager for existing patients already booked and patients for whom case records are created.

Surgsync checks the Xodus_Update column in the adt_pat_main and mri_pat_main tables for ADT updates. If a patient is updated in either table, Surgsync determines if the patient already exists in OR Manager. If the patient exists then the patient record in OR Manager is updated.

As transactions are filed in the Interface database (IDB), Surgsync checks each transaction and determines if it is associated with a medical record number (booking) or an account number (case record) that has been filed in the OR Manager database.

- All updates to demographic (medical record) data are filed for the patient's data. These are referenced by all bookings for that patient.
- Updates to information that is specific to an account number are filed for that particular account number only. Case records linked to that account number are updated only if they are open or re-opened. Closed case records are not updated because the case record is the legal documentation for each case—case records should reflect the exact information (even demographic data) of the patient at the time of surgery.

MM Updates

When using an MM Interface, Surgsync adds and updates stock items in OR Manager based on an audit date (table MM_ITEM_MAIN, column XODUS_UPDATE).

Surgsync processes all stock items available in OR Manager. Stock items are filed into OR Manager based on inventory. Before Surgsync processes stocks, SQL parameters must be setup to define the inventories to pull. When the parameters are set, Surgsync processes all stock items in the chosen inventories.

After all stock items are processed, Surgsync checks the xodus_update columns in the mm_item_main and mm_stock_main tables and updates stock items in OR Manager as necessary.

Billing and MM Reject Processing

Reject files track unsuccessful transmittals from OR Manager to your HCIS B/AR and MM systems.

- Reject files are automatically created when OR Manager is interfaced to Meditech HIS systems.
- Standard Billing and MM interfaces provide specifications for reject files.

- If reject files are sent from the billing or MM system to OR Manager, Surgsync processes them for viewing in OR Manager.
- Surgsync deletes reject files after they are processed.

Patient Record Merging

OR Manager supports medical record merges. When a merge is recorded via the ADT Interface, Surgsync performs a mirror merge of the patient in OR Manager.

Note: OR Manager does not currently support account number merges or relocations.

Surgsync Flags

The parameter flags for Surgsync are found in the file *Surgsyncflag.ini*. This table explains these flags.

Note: You should have a full understanding of how these flags work before modifying them.

Note: Settings included in the INI file but not documented below should retain their default value and not be edited.

Flag	Description	Standard Setting
Data_repo_type	The standard setting for linking into the Interface database.	Default setting is “Column” Do not change this setting
HCN_edit_ mask	Used only if flag USA = N. The formatting of Canadian Healthcare numbers in OR Manager.	####-###-###
Last_MM_Xodus_Update	For MM Interfaces, the date and time of the last batch processed. Last_MM_Xodus_Update is used when Surgsync is launched to determine the time from which to start MM updates.	You shouldn’t have to edit this date. However, you may adjust this flag if you need to reprocess a group of stock items and you know the “xodus” update date/time. The format has to be exactly as shown or Surgsync will not function. MM/DD/YYYY HH:MM:SS

Flag	Description	Standard Setting
LastXodusUpdate	For ADT Interfaces, the date and time of the last patient processed. LastXodusUpdate is used when Surgsync is launched to determine the time from which to start ADT updates.	You shouldn't have to edit this date. However, you may adjust this flag if you need to reprocess admissions and you know the xodus update date/time. The format has to be exactly as shown or Surgsync will not function: MM/DD/YYYY HH:MM:SS
MaxLedgerLines	The number of ledger lines that display in the Surgsync foreground application.	100 is the standard. This can be increased if necessary. **Note:** All lines displayed in the ledger are saved in medsurgledger text files.
Po_offset_days	Meditech sites only. Integer. If Process_po = Y this is the number of days in the past that POs be evaluated.	Standard setting is 30 days.

Process_po	Meditech sites only.
	Process POs for cost calculation.
		Y = process POs
		N = do not process POs

Save_stock_ errors	Stock update error logging. You may want to suppress logging if errors are being generated for known reasons. If an MM file does not supply the correct data components for cost, an error message is generated for every item that the cost cannot be calculated and set to zero.	Y = Surgsync will store errors in a log file N = Surgsync will not store errors

Flag	Description	Standard Setting
SecondsBetweenLoops	The number of second to pause Surgsync. Surgsync processing may use all available machine resources. Pausing releases machine resources and unlocks SQL tables to allow other processes to run.	120 seconds recommended. You may reduce to 15—30 seconds temporarily to speed Surgsync processing. ***Example:*** If Surgsync were off for a while and needed to catch up.

USA	Y / N	Y = United States hospital
		N = Non-US hospital

XodusRangeSeconds	If Surgsync is behind and catching up, XodusRangeSeconds specifies how many seconds the processing will jump ahead. If Surgsync were off for 8 hours, then turned back on, it would process where it left off. If there was nothing more to process, it would jump ahead this many seconds and continue to process during the next cycle.	1800 seconds (30 minutes) is the standard setting. Picis recommends that you do not change it.

Flag	Description	Standard Setting
current_time_minus_ seconds	If Meditech Extracts are used, a delay can be added to Surgsync so that MRI/ADT updates are not processed by Surgsync until after the Meditech Extracts process completely. Without a delay, Surgsync processes each update, which results in multiple updates to linked fields in bookings and case records. This setting is not included by default, so if needed it must be added manually.	Between 0 and 300 seconds.

Example: Sample *Surgsyncflag.ini* file

```
[Flags]
MaxLedgerLines=100
SecondsBetweenLoops=60
CDLSeconds=3600
Xodus_Range_Seconds=1800
Data_repo_type=column
LastXodusUpdate=03/01/2003 05:34:00
Last_MM_XodusUpdate=02/27/2003 12:00:00
Custom_data_lookups=03/05/2003 11:53:00
USA=Y
HCN_edit_mask=####-###-###
Save_stock_errors=Y
Process_po=Y
Po_offset_days=30
```

CareTaker and Surgsync

CareTaker should be configured to maintain Surgsync. (See *CareTaker* on page 43 for further details). Surgsync shuts down when either of the following conditions is satisfied:

- It is using more than 125 Mb of virtual memory.
- There has been no activity for more than seven minutes.

Configuring Surgsync autostart and monitoring options in CareTaker

1. Start **CareTaker**.
2. Click **Add Process** and browse to “C:\Picis\<ALIAS>\Surgsync\Surgsync.exe.”
3. Click **Open** and then click **Options**.
4. Under **Startup Options**, click **AutoStart** and **Start Minimized**.
5. Under **Monitoring Options** click **Monitor File Activity**.
6. Next to **File to Monitor** type the location of the *Surgsyncflag.ini* file: “C:\ProgramData\Picis\<ALIAS>\.”

Autoprint

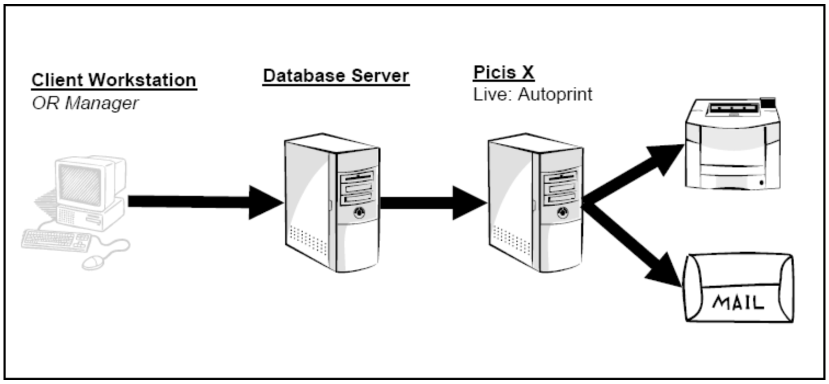
Autoprint is installed on two of the background servers. Its purpose is to publish changes for specified recipients via print or email. End-users enter criteria to determine under which conditions a notification should be sent.

This guide covers the technical configuration of Microsoft Outlook and OR Manager. For related information, please see the following guides:

- Installing Autoprint 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 *OR Manager User Guide*.

Autoprint Workflow

Client workstations using OR Manager are used to make changes to bookings or record events. These changes are stored in the database. Autoprint continually queries the database using pre-configured criteria. When a change is made to a booking or an event, Autoprint automatically sends a mail or printout notification.



See the application manuals for information about configuring the criteria that generates the notification.

Autoprint Configuration

All destinations (printers and email addresses) that will be used to send notifications need to be configured on the background server where Autoprint is installed.

Starting Autoprint

- At the Autoprint server, navigate to the folder “C:\Picis\<ALIAS>\Autoprint\” and double-click *Autoprint.exe* to start Autoprint.

Configuring printers for use with Autoprint

1. At the Autoprint server, install all Windows printers that will be required as destinations.
   - On the Start Menu, click **Printers and Faxes** and then click **Add Printer** under Printer Tasks. Follow the steps in the wizard. (For more information, consult your system administrator).
2. Start Autoprint and then click **Halt** to stop the queuing process.
3. Click **Maintenance** > **Destinations** (or click the Destinations maintenance button on the toolbar).

   The Destinations Maintenance window appears.
4. Click the **Import Printer** button.

   The Select Printer(s) window appears.
5. Select the box next to the printer(s) to be imported (as destinations) and then click **Import**.
6. Click **Save** and then click **Close**.

Configuring Email for use with Autoprint

1. At the Autoprint server, install Outlook.
2. Start Autoprint and then click **Halt** to stop the queuing process.

3. Click **Maintenance** > **Destinations** (or click the Destinations maintenance button on the toolbar).

   The Destinations Maintenance window appears.
4. Click the **Import Email** button.
5. Select the email addresses you want to import and then click **Import** to import email addresses to the destination list.
6. Click **Save** and then click **Close**.

Deleting a printer or email destination

This procedure shows how to remove (delete) a printer or email address from the destinations list.

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

1. Start Autoprint and then click **Halt** to stop the queuing process.
2. Click **Maintenance** > **Destinations** (or click the Destinations maintenance button on the toolbar).

   The Destinations Maintenance window appears.
3. Select a destination in the list and click **Delete**.

Autoprint Support

The main support task for Autoprint is ensuring that the application executable is started:

- Place Autoprint in the All Users start folder so any user who logs on will restart Autoprint.
- Use CareTaker to maintain Autoprint. (See *CareTaker* on page 43 for more details).

  Note: Autoprint will periodically stop based on a system variable that can be set for any number of minutes, from 0 (never shuts down) to infinity. The default is 30 minutes. (After Autoprint stops, CareTaker will restart it.)
- You should also implement procedures to be followed if the server stops responding.

Configuring Autoprint autostart options in CareTaker

1. Start **CareTaker**.
2. Click **Add Process** and navigate to “C:\Picis\<ALIAS>\Autoprint\Autoprnt.exe”.
3. Click **Open**.

   The process is added to the Caretaker window.
4. Click the **Options** button.

   The Options window appears.
5. Under Startup Options, select **Auto Start** and **Start Minimized** and then click **OK**.

6. In the Caretaker window, click the **Hide Form** button.

Autoprint Maintenance

Autoprint should be running at all times:

- If it is processing items in the queue, the processing queue status box displays the item that is currently being processed.
- If there are no items in the queue, the processing queue status box displays the message “Processing.”
- If Autoprint is not running, the processing queue status box will display the message “Halted.” Restart it by pressing the **Restart** button.

Troubleshoot Autoprint

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

Activating database logging

This procedure creates a file which logs Autoprint's database activity. The log file is session-specific, meaning each time the application is opened it overwrites any existing log file.

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

1. Close **Autoprint**.
2. At the Autoprint server, browse to the folder “C:\ProgramData\Picis\<ALIAS>” and double-click the file *Autoprnt.ini* to open it in Notepad.
3. Under the **Application** section, type the following parameters:

```
Sqlspy=yes
SqlspyLog=yes
```

4. Close and save *Autoprnt.ini*.
5. Restart Autoprint.

Deactivating database logging

1. Close **Autoprint**.
2. At the Autoprint server, browse to the folder “C:\ProgramData\Picis\<ALIAS>” and double-click the file *Autoprnt.ini* to open it in Notepad.
3. Under the **Application** section, delete the following parameters:

```
Sqlspy=yes
SqlspyLog=yes
```

4. Close and save *Autoprnt.ini*.
5. Restart Autoprint.

> **Note:** You can also comment the parameters out by adding a semi-colon (;) before each line.

Viewing the autoprntsqlspylog.txt database logging file

This procedure assumes that the background server has database logging activated (See *Activating database logging* on the previous page for further details).

- At the Autoprint server, browse to the folder “C:\ProgramData\Picis\<ALIAS>” double-click the file *autoprntSqlSpylog.txt* to open it in Notepad.

Activating Autoprint booking sheet logging

This procedure creates a log file (*Booksheet_print_queue_debug.tx*t) of how OR Manager decides to send bookings to Autoprint's queue.

> **Note:** The log file should be deactivated when no troubleshooting is needed because it can cause the application to run slower.

- In the PSM database, set the “booksheet_print_queue_debug” systemflag for application name as follows: `medsurg=Y`.

  To confirm logging is activated, create and file a new booking in OR Manager to send at least one job to Autoprint, or edit an existing booking.

  Exit the booking and check to see if Autoprint printed the job. If not, view the log file.

Deactivating Autoprint booking sheet logging

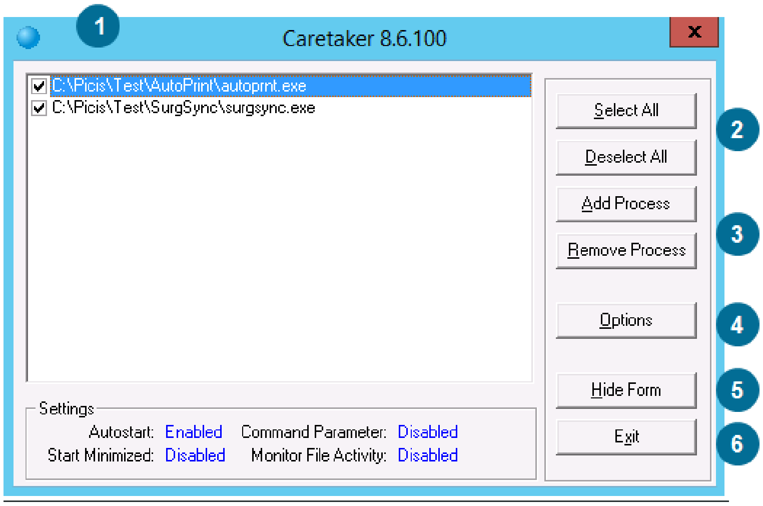
- In the PSM database, set the “booksheet_print_queue_debug” systemflag to N.

Viewing the booksheet_print_queue_debug.txt logging file

- At the OR Manager workstation, browse to the "Bin" folder and double-click the file *Booksheet_print_queue_debug.txt* to view it in Notepad.

CareTaker

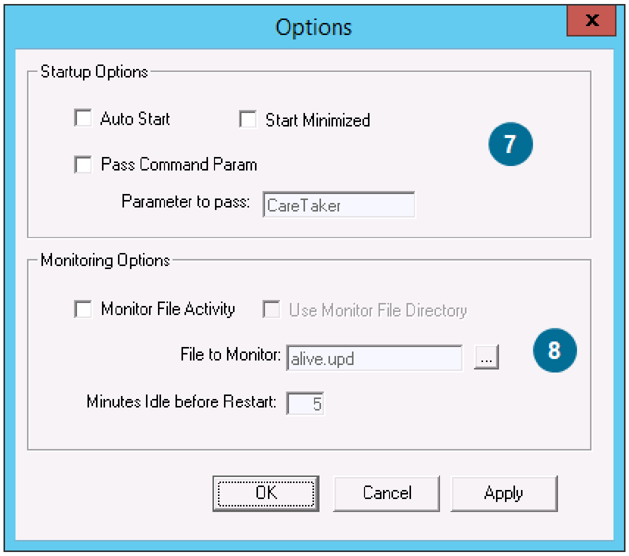
CareTaker is used to maintain background applications (.exe files) to ensure they are constantly in an active state. CareTaker minimizes maintenance by automatically restarting these applications when they close. CareTaker has the following options.



☑ C:\Picis\Test\AutoPrint\autoprnt.exe
☑ C:\Picis\Test\SurgSync\surgsync.exe

Settings
Autostart: Enabled Command Parameter: Disabled
Start Minimized: Disabled Monitor File Activity: Disabled

1. **Monitor Executable**: Multiple executables can be maintained simultaneously.
2. **Select Executable**: Executables that are selected will start. Executables that are not selected will be stopped.
3. **Add Processes**: Executable can be added and removed.
4. **Options**: Each executable can be specifically configured using options.
5. **Hide Form**: CareTaker is started but running in the background with the icon visible in the task bar.
6. **Exit**: Close CareTaker.


Options

Startup Options

☐ Auto Start ☐ Start Minimized

☐ Pass Command Param

Parameter to pass: CareTaker

Monitoring Options

☐ Monitor File Activity ☐ Use Monitor File Directory

File to Monitor: alive.upd

Minutes Idle before Restart: 5

7. **Startup Options**: Configure the startup option for CareTaker:
   - **AutoStart**—Determines if all selected executable are started when CareTaker starts. (it is recommended this is always selected.)
   - **Start Minimized**—Determines if all selected executable are started minimized.
   - **Pass Command Parameter**—Allows command line parameters to be passed to the executable.
8. **Monitoring Options**: Configure the file options for CareTaker:
   - **Monitor File Activity**—Denotes a file will be maintained
   - Use Monitor File Directory—Directory where monitored file exists
   - **File to Monitor**—Type the name of the file
   - **Minutes Idle before Restart**—Number of minutes the file will be without activity before CareTaker restarts the application.

Note: Startup options and monitoring options are set once for all processes that are in this instance of CareTaker. If necessary, multiple instances of CareTaker can be running to allow different configurations.

The following background applications need to be maintained by CareTaker:

Executable Name	Background Application
C:\Picis\<ALIAS>\Autoprint\Autoprint.exe	Autoprint
C:\Picis\<ALIAS>\Surgsync\Surgsync.exe	Surysync

CareTaker tracks the Windows process identifier for each process added to the process list. When CareTaker starts a process, it records the associated process identifier that Windows assigns to the process. The status of the process identifiers are then checked every five seconds. If any of the maintained processes stops, and therefore loses its previously assigned process identifier, CareTaker will restart that process.

Note: CareTaker should be added to the startup folder of the logged on user. This will allow CareTaker to start when the background server starts.

Starting CareTaker

- Double-click the **CareTaker** icon on the desktop.

  Or

- Browser to the folder “C:\Picis\<ALIAS>\CareTaker” and double-click *CareTaker.exe*. (Assuming that CareTaker is installed in the default folder).

Hiding CareTaker in the Task Bar

- Click **Hide Form** in the CareTaker window.

Opening CareTaker from the Task Bar

CareTaker is started but hidden in the task bar.

- From the task bar, double-click the CareTaker icon (blue bubble).

Closing CareTaker

- Click **Exit**.

  Or

- Click the **X** in the top right-hand corner.

Adding an Executable File

1. Start **CareTaker** then click **Add Process** and navigate to the executable file to be added.
2. Click **Open**.
3. Select the box next the executable file to be added.

Starting an executable file

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

1. From the task bar, double-click the CareTaker icon (blue bubble) or start CareTaker.
2. Select the box next to the executable file to be started.

Stopping an executable file

Use this procedure to stop any of the transaction processors.

1. From the task bar, double-click the CareTaker icon (blue bubble).
2. Clear the box next to the executable file to be stopped.

Configuring startup options

1. Start **CareTaker** and click **Options**.
2. Select the box next any of the following options:

- **AutoStart**: Determines if all selected executable are started when CareTaker starts. (Picis recommends this is always selected).
- **Start Minimized**: Determines if all selected executable are started minimized.
- **Pass Command Parameter**: Allows command line parameters to be passed to the executable.

Configuring monitoring options

1. Start **CareTaker** and click **Options**.
2. Select the any of the following options:
   - **Monitor File Activity**: Denotes a file will be monitored.
   - **Use Monitor File Directory**: Specifies the directory when monitoring is used for Autoprint and Surgsync while Meditech Extracts exist on the same machine.
   - **File to Monitor**: Type the name of the file.
   - **Minutes Idle before Restart**: Number of minutes the file will be without activity before CareTaker restarts the application.

Configuring CareTaker to start automatically

1. Navigate to the folder “C:\Picis\<ALIAS>\CareTaker.”

   (Assuming CareTaker is installed in the default folder).
2. Right-click *CareTaker.exe* and select **Create Shortcut**.
3. Right-click *Shortcut to CareTaker.exe* and select **Cut**.
4. Navigate to the Start Menu programs folder: “C:\ProgramData\Microsoft\Windows\Start Menu\Programs.”
5. Right-click in the folder and select **Paste**.

Configure Caretaker for Meditech Extracts at Machine with Autoprint and Surgsync

For sites using the Monitor File Activity option in CareTaker for Autoprint and Surgsync, and also using CareTaker for Meditech Extracts on the same machine, separate directories must exist for each purpose.

After CareTaker has been installed and configured for Autoprint and Surgsync, follow these steps to configure CareTaker for use with Meditech Extracts (if CareTaker is used for both on the same machine).

Creating a CareTaker directory for Meditech Extracts

1. Browse to the folder "C:\Picis\<ALIAS>" and create a copy of the "CareTaker" folder.
2. Rename the new folder as "CareTakerExtracts."

   This is the directory that is designated for use with Extracts.

3. In the "CaretakerExtracts" folder, double-click the file *CareTaker.exe* to start Caretaker.
4. Click the **Add Process** button and add the Extracts to this instance of CareTaker.

   Now you should have one instance of CareTaker configured to manage Autoprint and Surgsync and another instance of CareTaker configured to manage Extracts.

Configuring file monitoring Autoprint and Surgsync with multiple CareTaker directories

1. Browse to the folder "C:\Picis\<ALIAS>\CareTaker" and start CareTaker.
2. Click the **Options** button.
3. Under Monitoring Options, select the **Monitor File Activity** checkbox and the **Use Monitor File Directory** checkbox.
4. In the **File to Monitor** field, type the name of the file to monitor.
5. Click **OK** and close or minimize the CareTaker window.

4

Reporting with Crystal Reports

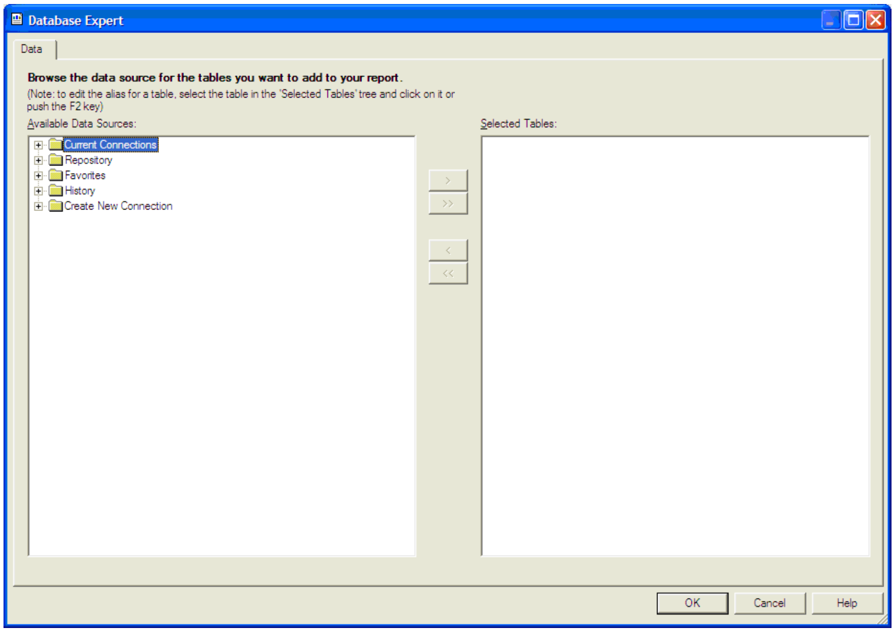
Connecting to Crystal Reports

Crystal Reports should be connected to the ORM database via OLE(ADO).

1. Start Crystal Reports.
2. Click **File** > **New**.

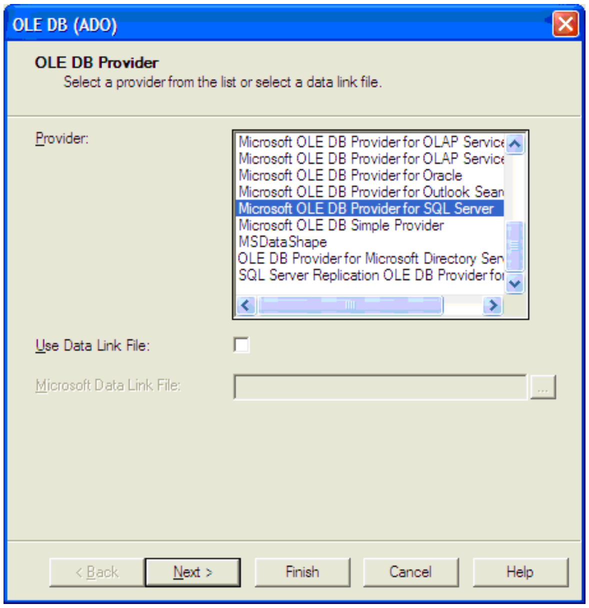
   The Crystal Reports Gallery window appears.
3. Select **Using the Report Wizard** and click **Next**.

   The Database Expert window appears.



Browse the data source for the tables you want to add to your report.
(Note: to edit the alias for a table, select the table in the 'Selected Tables' tree and click on it or push the F2 key)

4. Double-click **Create New Connection**, navigate to **OLE DB (ADO)**.
5. Double-click **Make New Connection**.
   The following window appears.



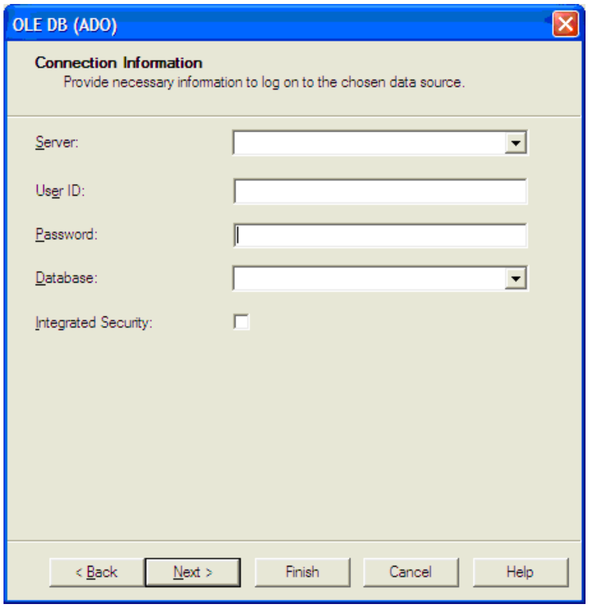
OLE DB Provider
Select a provider from the list or select a data link file.

Provider:
Microsoft OLE DB Provider for OLAP Service
Microsoft OLE DB Provider for OLAP Service
Microsoft OLE DB Provider for Oracle
Microsoft OLE DB Provider for Outlook Sear
Microsoft OLE DB Provider for SQL Server
Microsoft OLE DB Simple Provider
MSDataShape
OLE DB Provider for Microsoft Directory Ser
SQL Server Replication OLE DB Provider fo

Use Data Link File: ☐

Microsoft Data Link File:

6. Select **Microsoft OLE DB Provider for SQL Server** and click **Next**.
   The following window appears.



7. Specify the following details in the corresponding boxes:
   a In **Server**, select your OR Manager server from the drop-down box or type the IP address.
   b In **User ID**, enter the user name for the physical user.

> **Note:** In previous releases, the reportuser database login was delivered. That login will remain in place and usable if it was at your site in a previous release, but reportuser is no longer delivered or supported. This is to ensure compliance with security protocols. When you create external Crystal Reports, use a database user that has read-only access to the application databases.

   c In **Password**, enter the user name for the physical user.
   d In **Database**, select your OR Manager database from the drop-down box.

8. Click **Next**.

   The Advanced Information window appears.

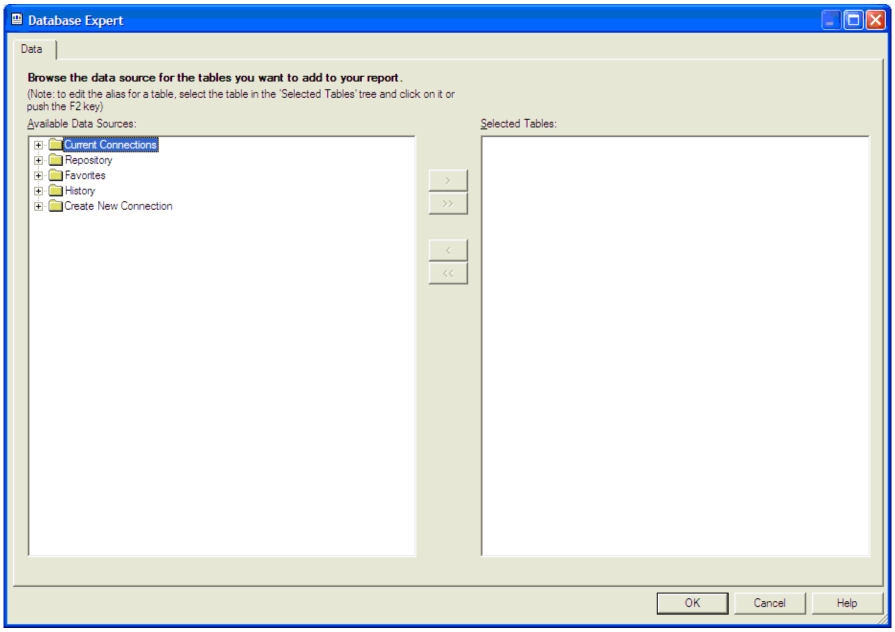
9. Click **Finish** to complete the wizard.

Selecting Tables for a Report

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

1. Start Crystal Reports.
2. From the **File** menu click **New**. The Crystal Report Gallery window appears.
3. Select **Using the Report Wizard** and click **Next** (you could also select a Blank Report).

The Database Export window appears.



Browse the data source for the tables you want to add to your report.

(Note: to edit the alias for a table, select the table in the 'Selected Tables' tree and click on it or push the F2 key)

4. Double-click **Current Connections** and navigate to **OLE DB(ADO)** and then click the Server name of the connection you created.
5. Highlight a table or view and click the **>** button to select the table.
6. Click **OK** to complete.

5

Activity Logs & Diagnostic Tools

Log and Diagnostic Tools Overview

Picis Perioperative and Critical Care includes methods for logging application activity and a variety of useful diagnostics tools. Below is a list of these tools, with details on where you can find more information on the tool.

The diagnostics tools are available at both workstations and servers:

- **Windows Server** - “C:\Picis\Diagnostics” folder
- **Windows Desktop** - “C\Program Files (x86)\Bin” folder

Log files are typically stored in the following workstation folder:

- “C:\ProgramData\PICIS\<ALIAS>”

This chapter includes descriptions of the following diagnostics tools:

- *SqlSpy Logs* on the next page
- *ADT Administrator* on page 63
- *CNLSpy* on page 63
- *Picis Configuration Wizard* on page 139
- *HL7InterfaceTest* on page 63
- *HL7 Outbound Messaging Log* on page 63
- *NKTSpy* on page 63
- *PcmExportTestClient* on page 64

- *PCMTestClient* on page 64
- *Perfect Trace* on page 56
- *Messaging Spy* on page 64

SqlSpy Logs

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

- OR Manager
- SmarTrack
- Security Manager
- Surgsync
- Autoprint

SqlSpy can record the following types of application activity:

- **SqlSpy log**: This records all SQL statements sent from the host machine to application's database.
- **Debug logs**: This records application commands that can be interpreted by a developer.

Note: Unlike Perfect Trace, there is no executable file for SqlSpy — the logs are activated from within OR Manager.

Logs depend on the session. Once activated, the log file will be populated with messages until the application is closed or the log files 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 on workstations and servers: "C:\ProgramData\PICIS\<ALIAS>."

The file format is as follows:

- On a client workstation:
  - *medsurgSqlSpylog_YYYYMMDD HHMMSS.txt*
- On a Citrix server:
  - *medsurgSqlSpylog<CitrixIPAddress>_YYYYMMDD HHMMSS.txt*

Activating the SqlSpy log

◆ In OR Manager, click **Tools** > **Options** > **SQLSpy On**.

An icon is visible in the toolbar when logging is active.

Deactivating the SqlSpy log

- In OR Manager, click **Tools** > **Options** > **SQLSpy Off**.

Activating the Debug log

- In OR Manager, click **Tools** > **Options** > **DebugLog On**.
  An icon is visible in the toolbar when logging is active.

Deactivating the Debug log

- In OR Manager, click **Tools** > **Options** > **DebugLog Off**.

SQL Log Traces

When SQL log traces are active, the traces are logged to files. To help with troubleshooting, you can save a capture file or you can view a log file as you perform actions in the application.

Note: The first entries in a log file are from the ini file used by OR Manager.

Saving the SqlSpy log

1. In OR Manager, click **Tools** > **Options** > **SQLSpy Capture**.
2. Type the name of the file in the space provided and click **OK**.

Saving the Debug log

1. In OR Manager, click **Tools** > **Options** > **DebugLog Capture**.
2. Type the name of the file in the space provided and click **OK**.

Viewing the SqlSpy log and/or Debug log with the application open

1. Close OR Manager, if it is not already closed.
2. Browse to the folder “C:\ProgramData\Picis\<ALIAS>” and open the file *Medsurg.ini* using a text editor (such as Notepad).
3. Add the following parameters under the `Application` section:

```
SqlSpyWindow=yes
SqlSpyOnTop=yes
```

   Note: `SqlSpyOnTop` is optional; it keeps the window in view.

4. Save and close the file *Medsurg.ini*.

5. Open OR Manager and activate one of the log files. (See *Activating the SqlSpy log* on page 54 or *Activating the Debug log* on the previous page for further information).

   When you use OR Manager the traces will be visible in a window.

Perfect Trace

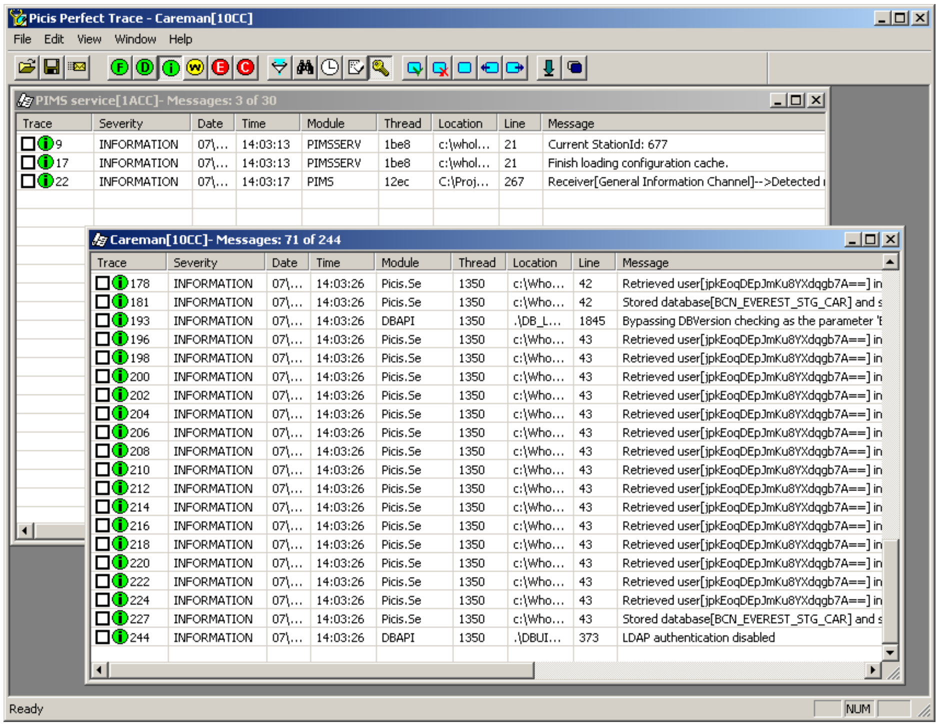
Perfect Trace is a diagnostic tool used to log Perioperative and Critical Care application and background services activity. Perfect Trace can be used to audit the following applications and services:

- Anesthesia Manager, PACU Manager, or Critical Care Manager
- Preop Manager
- Clinical Notes System
- The PCM service

Note: Users will need the “Diagnostics Tools” system right to open Perfect Trace. See your Picis system administrator if you are not able to open Perfect Trace.

Getting Started

When Perfect Trace is open it automatically records application activity for all compatible applications that are started on that workstation. Perfect Trace opens one window for each Perioperative and Critical Care module or process started on the workstation or server. In the graphic above, two modules are open on the workstation.



PIMS service[1ACC]- Messages: 3 of 30

Trace	Severity	Date	Time	Module	Thread	Location	Line	Message
□ 9	INFORMATION	07\...	14:03:13	PIMSSERV	1be8	c:\whol...	21	Current StationId: 677
□ 17	INFORMATION	07\...	14:03:13	PIMSSERV	1be8	c:\whol...	21	Finish loading configuration cache.
□ 22	INFORMATION	07\...	14:03:17	PIMS	12ec	C:\Proj...	267	Receiver[General Information Channel]-->Detected

Careman[10CC]- Messages: 71 of 244

Trace	Severity	Date	Time	Module	Thread	Location	Line	Message
□ 178	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	42	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 181	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	42	Stored database[BCN_EVEREST_STG_CAR] and s
□ 193	INFORMATION	07\...	14:03:26	DBAPI	1350	.\DB_L...	1845	Bypassing DBVersion checking as the parameter 'I
□ 196	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 198	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 200	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 202	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 204	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 206	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 208	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 210	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 212	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 214	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 216	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 218	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 220	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 222	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 224	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Retrieved user[jpkEoqDEpJmKu8YXdqgb7A==] in
□ 227	INFORMATION	07\...	14:03:26	Picis.Se	1350	c:\Who...	43	Stored database[BCN_EVEREST_STG_CAR] and s
□ 244	INFORMATION	07\...	14:03:26	DBAPI	1350	.\DBUI...	373	LDAP authentication disabled

Typically, Perfect Trace is used to record application activity when abnormal behavior is being observed. The following workflow would be used:

1. Open Perfect Trace on the Workstation/Server.
2. Start the application/service you want to troubleshoot.
3. Perform the steps required to see the abnormal behavior.
4. Save the Perfect Trace file and send it to Picis Support.

Perfect Trace, when running in this interactive mode, stores logging information in memory. During extended periods (three to four hours) of logging, using Perfect Trace, a deterioration in workstation/server performance might be noticed. Closing Perfect Trace and reopening solves this problem. As you work with Perfect Trace, you should conduct your own testing to verify the length of time Perfect Trace can be used without causing performance problems.

Starting Perfect Trace

1. Open Perfect Trace by double-clicking the file *PerfectTrace.exe* in one of the folders below:

   Windows Server- “C:\Picis\Diagnostics”
   Windows 7- “C:\Program Files (x86)\Picis\Bin”
2. Enter a valid user name and password to log on.

Closing Perfect Trace

- Click **File** menu > **Exit**.

Saving a Perfect Trace file

1. Start **Perfect Trace**.
2. Select a window.
3. Click **File** > **Save**.
4. In the space provided enter a file name and click **Save**.

   The active window is saved as a file with the extension .DBG.

Display Settings

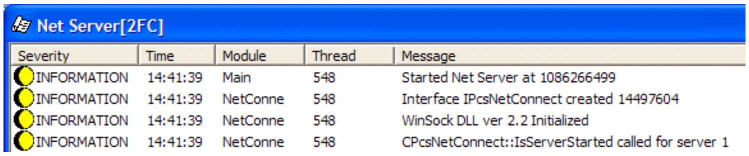
By default, a maximum of 50,000 lines are visible in each window. This means if the file you are viewing contains more than this limit they will not be visible.

Changing the viewing resolution

1. Start **Perfect Trace**.
2. Select a window.
3. Click **View** > **Maximum displayed messages**.
4. In the space next to **Maximum messages** enter a numeric value.
5. Click **OK** when you have finished.

Perfect Trace Messages

Perfect Trace displays the following information for each message:



Severity	Time	Module	Thread	Message
INFORMATION	14:41:39	Main	548	Started Net Server at 1086266499
INFORMATION	14:41:39	NetConne	548	Interface IPcsNetConnect created 14497604
INFORMATION	14:41:39	NetConne	548	WinSock DLL ver 2.2 Initialized
INFORMATION	14:41:39	NetConne	548	CPcsNetConnect::IsServerStarted called for server 1

- **Severity**: Severity rating attached to the message. It will be either, Information, Critical, Error, Debug, or Full Debug.
- **Time**: The time the message was recorded.
- **Module**: Source module.
- **Thread**: Source thread.
- **Message**: Text of the message.

Viewing a Perfect Trace message detail

1. In Perfect Trace, double-click a message.

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

2. Click **OK** when you have finished.

View Perfect Trace Files

Perfect Trace 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.

Viewing a Perfect Trace file at run-time

Perfect Trace files can be viewed at the same time as the application sends messages to the file.

- Start Perfect Trace and then start an application.

  The file is displayed.

Viewing a Perfect Trace file

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

   The file is displayed.

Filtering by severity

Each message in Perfect Trace is assigned one of the following severities: Critical, Error, Information, Debug, or Full Debug.

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

1. Start **Perfect Trace**.
2. Click **View** > **Filter**.
3. From the Severity drop-down menu, select a filter e.g. Full Debug.
4. Click **OK** to return to the results window.

Filtering by traces, modules, threads, files and lines

For Traces, Modules, Threads, Files and Lines, filter criteria can be set that can either be excluded or included.

1. Start **Perfect Trace**.
2. Click **View** > **Filter**.
3. In the appropriate box type the search text.
4. If this is to be excluded select the box next to **Exclude**.
5. Click **OK** to return to the results window with the filter applied.

Filtering by messages

Filters can be applied to message text. This is particularly useful when you want to view a specific Patient or Admission on the PCM server.

1. Start **Perfect Trace**.
2. Click **View** > **Filter**.
3. In the box next to Include Messages or Exclude Messages type the search text.
4. Select the box next to **Satisfy all Criteria** to search for a complete match.
   (With this option selected, Gold would return only Gold whereas with this option cleared, Gold would return Goldsmith, Goldthorp and Goldstein).
5. Select the box next to **Ignore case** to search regardless of case.
   (With this option selected, Gold would return only Gold whereas with this option cleared, Gold would return gold, GOLD and GOld).
6. Click **OK** to return to the results window with the filter applied.

Automatic Perfect Trace Files

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

- **Windows 7**- “C:\ProgramData\Picis\<ALIAS>”
- **Windows Server**- “C:\ProgramData\Picis\<ALIAS>\<FolderName>”

Activating automatic Perfect Trace file collection

1. Close Perfect Trace, if necessary.
2. Browse to a location below and open the file *RegistrySettings.config*.

   Windows 7- “C:\Program Files (x86)\Picis\Bin”
   Windows Server- “C:\Picis”
3. Edit these settings as follows:

```
LogToFile="true"
FolderName="<name of the folder for trace files>"
```

Note: Only enter the folder where trace files should be saved, not the entire path to the folder.

4. Close and save the file.

   The next time an application is started, trace files are automatically saved to the folder you’ve specified, in one of the following locations:

   Windows 7- “C:\ProgramData\Picis\<ALIAS>\<FolderName>”
   Windows Server-“C:\ProgramData\Picis\<ALIAS>\<FolderName>”

Changing the trace file destination

1. Close Perfect Trace, if necessary.

2. Browse to a location below and and open the file *RegistrySettings.config*.

   Windows 7- “C:\Program Files (x86)\Picis\Bin”
   Windows Server- “C:\Picis”
3. Edit the FolderName setting to specify the new folder for trace files.

   > **Note:** Only enter the folder where trace files should be saved, not the entire path to the folder.
4. Close and save the file.

   The next time an application is started, trace files are automatically saved to the folder you’ve specified, in one of the following locations:

   Windows 7- “C:\ProgramData\Picis\<ALIAS>\<FolderName>”
   Windows Server- “C:\ProgramData\Picis\<ALIAS>\<FolderName>”

Perfect Trace Log File Maintenance

Perfect Trace log files are not automatically purged; however, a utility called PtLogCleaner is provided to periodically purge these files. Using PtLogCleaner, you can purge log files on an ad-hoc basis by executing a command, or you can establish a scheduled purge to delete files that are older than a particular number of days that you configure.

With each option, you can specify the folder from which log files should be deleted. The folder parameter is optional. If a folder is not specified, log files are deleted from the default logging folder, which is configured with the `FolderName` value in the *RegistrySettings.config* file. For more information, see *Automatic Perfect Trace Files* on the previous page.

> **Note:** Administrative rights are required to configure PtLogCleaner.

Manually purge files older than # of 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 (x86)\Picis\Bin\PtLogCleaner.exe [-days <*NumberOfDays*>] [-folder <*Folder*>]”
   Windows Server- “C:\Picis\Diagnostics\PtLogCleaner.exe [-days NumberOfDays] [-folder Folder]”

   Where <NumberOfDays> specifies the number of days over which log files will be deleted; files older than this number are deleted, and

   <Folder> is the folder where the log files are stored (this is optional; exclude to use the default location).
3. Press **ENTER**.

Schedule an automated log file purge

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

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

   Windows 7- “C:\Program Files (x86)\Picis\Bin\PtLogCleaner.exe -install Time [<*User*>] [-days <*NumberOfDays*>] [-folder <*Folder*>]"
   Windows Server- “C:\Picis\Diagnostics\PtLogCleaner.exe -install Time [<*User*>] [-days <*NumberOfDays*>] [-folder <*Folder*>]”

   Where <User> is the current user name and,

   <NumberOfDays> specifies the number of days over which log files will be deleted; files older than this number are deleted, and

   <Folder> is the folder where the log files are stored (this is optional; exclude to use the default location).
3. Press **ENTER**.

Converting a Perfect Trace log file to a text file

1. Open Command Prompt using **Run as Administrator**.
2. Type one of the following commands, depending on your machine:

   Windows 7- “C:\Program Files (x86)\Picis\Bin\PtLogCleaner.exe –convert <File Path and Filename>”
   Windows Server-“C:\Picis\Diagnostics\PtLogCleaner.exe **–convert <File Path and Filename>**”

   where <File Path and Filename> are the original file’s path and name.
3. Press **ENTER**.

   The command prompt window remains open after the text file is created.

Perfect Trace Configuration

Perfect Trace (when in automatic mode) records large amounts of information, which can use up a lot of hard disk in a short time period of time. Two configuration parameters are available to manage these files.

- **Max File Numbers:** Dictates the maximum number of perfect trace files for an application. Default = 5 (files).
- **Max File Length:** The maximum file size expressed in bytes. Default 8388608 (8 x 1024 x 1024).

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

Assuming the default configuration, the behavior will be as follows:

1. The first file is populated until it reaches a size of 8388608 bytes.
2. A second is created until it reaches a size of 8388608 bytes.
3. A third, fourth and fifth file are created and populated until they reach a size of 8388608 bytes.
4. When the fifth file reaches a size of 8388608 bytes, the first file is overwritten and the cycle begins again.

HL7 Outbound Messaging Log

The HL7 Outbound Messaging Log is available to view messages sent via PCM.NET. Using the Messaging Log, you can view the status of outbound messages, and attempt to resend those that have not be exported successfully.

Special configuration is required to enable the Messaging Tool. For more information, see *HL7 Outbound Messaging Log* on page 73.

ADT Administrator

ADT Administrator is used to configure census windows for Anesthesia Manager, PACU Manager, Critical Care Manager, Preop Manager, CaseCheck, and the Printouts Viewer, as well as perform a variety of management functions on patient records.

Detailed information on ADT Administrator is available in the *System Configuration Guide* and *Workstation User Guide*.

CNLSpy

This tool is used to test Clink'n Link driver connectivity. For more information, see *Device Drivers* on page 92.

HL7InterfaceTest

HL7InterfaceTest is used to test Interface activity.

NKTSpy

This tool is used to test NKT driver connectivity. For more information, see *Device Drivers* on page 92.

PcmExportTestClient

The PCM Export Test Client can be used to verify that the PCM export has been properly installed and configured, and to diagnose problems. This tool is described in the *PCM Manual*.

PCMTestClient

The PCM Import Test Client (also known as the PCM Test Client) can be used to verify that the PCM import has been properly installed and configured, to diagnose problems and to validate third-party export clients. This tool is described in the *PCM Manual*.

Messaging Spy

You can use Messaging Spy to check that the network messages related to the PCM server are created correctly.

Picis (web) Services Diagnostics

The Picis (web) Services offer logging capabilities as well as advanced diagnostics options for troubleshooting.

- *Picis (web) Services Logging Capabilities* below
- *Picis (web) Services Diagnostics Logging Capabilities* on page 70

Picis (web) Services Logging Capabilities

Each of the Picis (web) Services has a *web.config* file which, among other things, controls the amount and location of logging information. The `categorySources` section of the *web.config* file includes the following traces, which can be configured for logging in the Picis (web) Services log directory, the Windows Event Viewer Application log, or both:

- Critical Error
- Error
- Warning

- Information
- Debug
- Full Debug

All of these trace categories are available in the *web.config* file, and logging activity is controlled by enabling or disabling the trace activities for the Picis (web) Services.

Log to a Picis (web) Services Log Directory

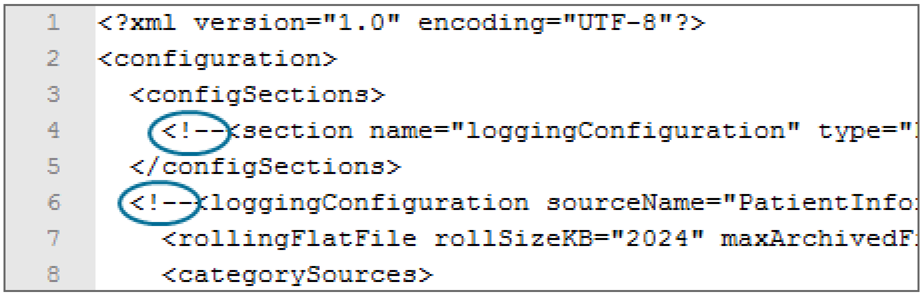
The setting that controls Picis (web) Services logging is called Flat File Destination, and this is enabled by default for the following traces:

- Critical Error
- Error
- Warning

You can add more traces or remove traces to adjust the amount of logging by editing the `listeners` section of the *web.config* file for the trace you want to include or exclude.

Adding traces for Flat File Destination logging

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. To enable edits to the logging configuration, edit line 4 to remove the opening (<!--) and closing (-->) comment tags, and remove the opening comment tag from line 6 and corresponding closing tag from line 43.

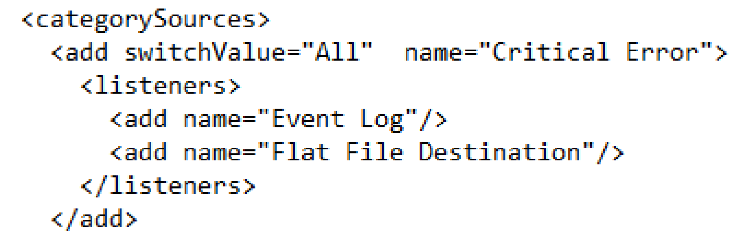


```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <configuration>
3    <configSections>
4      <!--<section name="loggingConfiguration" type="
5    </configSections>
6    <!--<loggingConfiguration sourceName="PatientInfo
7      <rollingFlatFile rollSizeKB="2024" maxArchivedF
8      <categorySources>
```

4. Add the following entry in the `listeners` section for the trace(s) you want to enable:

```
<add name="Flat File Destination"/>
```

Example: In the example below, Critical Error logging is enabled with the addition of `Flat File Destination`:



```
<categorySources>
  <add switchValue="All"  name="Critical Error">
    <listeners>
      <add name="Event Log"/>
      <add name="Flat File Destination"/>
    </listeners>
  </add>
```

5. Save and close the *web.config* file.

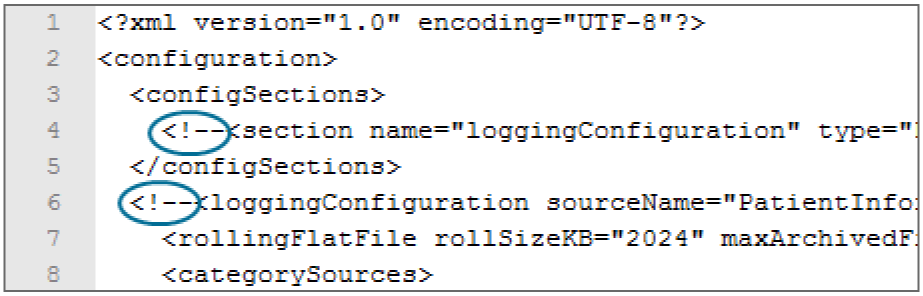
   The log file is created in the following location:

   “<IIS base path>\wwwroot\<service name>Service\Log\FileTraceTest.log”

   where <IIS base path> is typically “C:\inetpub”

Removing traces from Flat File Destination logging

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. To enable edits to the logging configuration, edit line 4 to remove the opening (<!--) and closing (-->) comment tags, and remove the opening comment tag from line 6 and corresponding closing tag from line 43.

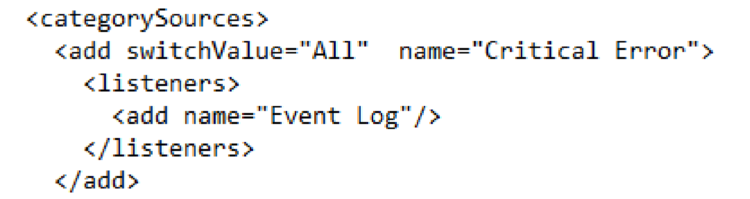


```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <configuration>
3    <configSections>
4      <!--<section name="loggingConfiguration" type="
5    </configSections>
6    <!--<loggingConfiguration sourceName="PatientInfo
7      <rollingFlatFile rollSizeKB="2024" maxArchivedF
8      <categorySources>
```

4. Remove the following entry in the `listeners` section for the trace(s) you want to disable:

```
<add name="Flat File Destination"/>
```

Example: In the example below, Critical Error logging is disabled with the absence of `Flat File Destination`:



```
<categorySources>
  <add switchValue="All"  name="Critical Error">
    <listeners>
      <add name="Event Log"/>
    </listeners>
  </add>
```

5. Save and close the *web.config* file.

   The log file is created in the following location:

   “<IIS base path>\wwwroot\<service name>Service\Log\FileTraceTest.log”

   where <IIS base path> is typically “C:\inetpub”

Log to Microsoft Event Viewer Application

Microsoft Event Viewer logging is enabled by default. There are two trace levels available for logging to the Event Viewer: Event Log and Basic Event log.

Default logging traces for Windows Event Viewer Event log:

- Critical Error
- Error

Default logging traces for Windows Event Viewer Basic Event log:

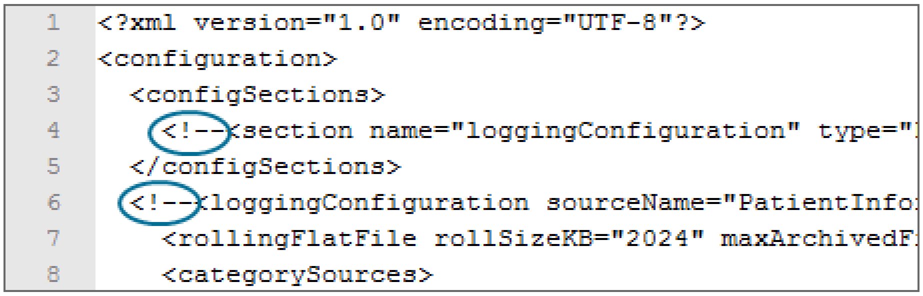
- Warning
- Information
- Debug
- Full Debug

You can add more traces or remove traces to adjust the amount of logging by editing the `listeners` section of the *web.config* file for the trace you want to include or exclude.

The size and number of files created in the Windows Event Viewer log are limited to 2024KB and 100 files, respectively. These settings are configured in the `loggingCongiuration` section of the *web.config* file for each of the Picis (web) Services.

Adding traces for Event Viewer logging

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. To enable edits to the logging configuration, edit line 4 to remove the opening (<!--) and closing (-->) comment tags, and remove the opening comment tag from line 6 and corresponding closing tag from line 43.



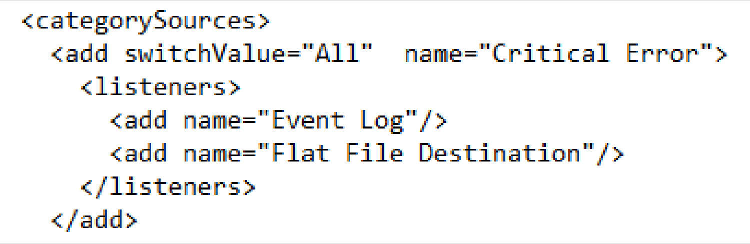
```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <configuration>
3    <configSections>
4      <!--<section name="loggingConfiguration" type="
5    </configSections>
6    <!--<loggingConfiguration sourceName="PatientInfo
7      <rollingFlatFile rollSizeKB="2024" maxArchivedF
8      <categorySources>
```

4. Add one of the following entries in the `listeners` section for the trace(s) you want to enable:

```
<add name="Event Log"/>

<add name="Basic Event Log"/>
```

> ***Example:*** In the example below, Critical Error logging is enabled with the addition of `Event Log`:

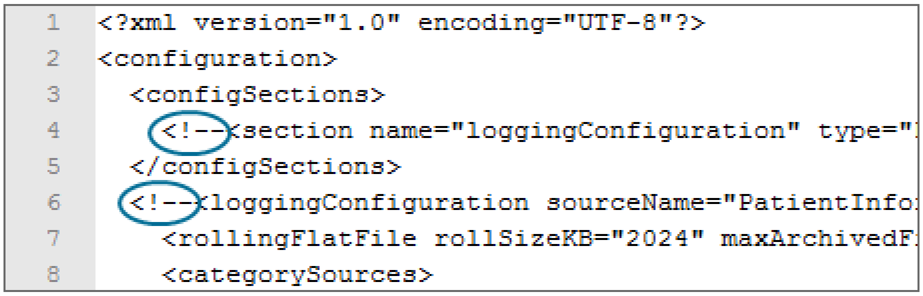


```
<categorySources>
  <add switchValue="All"  name="Critical Error">
    <listeners>
      <add name="Event Log"/>
      <add name="Flat File Destination"/>
    </listeners>
  </add>
```

5. Save and close the *web.config* file.

Removing traces from Event Viewer logging

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. To enable edits to the logging configuration, edit line 4 to remove the opening (<!--) and closing (-->) comment tags, and remove the opening comment tag from line 6 and corresponding closing tag from line 43.



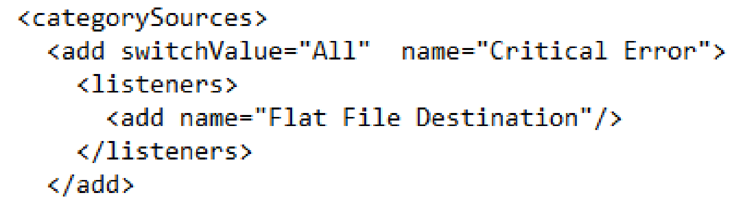
```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <configuration>
3    <configSections>
4      <!--<section name="loggingConfiguration" type="
5    </configSections>
6    <!--<loggingConfiguration sourceName="PatientInfo
7      <rollingFlatFile rollSizeKB="2024" maxArchivedF
8      <categorySources>
```

4. Add or remove one of the following entries in the `listeners` section for the trace(s) you want to disable:

```
<add name="Event Log"/>

<add name="Basic Event Log"/>
```

> ***Example:*** In the example below, Critical Error logging is disabled with the absence of `Event Log`:



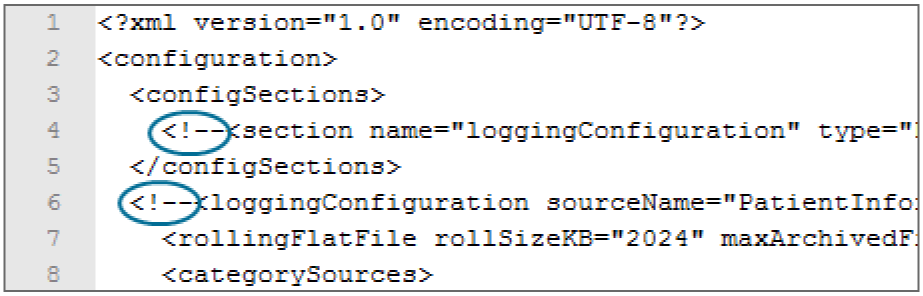
```
<categorySources>
  <add switchValue="All"  name="Critical Error">
    <listeners>
      <add name="Flat File Destination"/>
    </listeners>
  </add>
```

5. Save and close the *web.config* file.

Configuring File Size in Microsoft Event Viewer Application

A limited number of log files are created per service. These default settings are specified in the *web.config* file for each of the Picis (web) Services, and can be modified to adjust the maximum file size and number of archive files allowed.

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. To enable edits to the logging configuration, edit line 4 to remove the opening (<!--)and closing (-->) comment tags, and remove the opening comment tag from line 6 and corresponding closing tag from line 43.



```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <configuration>
3    <configSections>
4      <!--<section name="loggingConfiguration" type="
5    </configSections>
6    <!--<loggingConfiguration sourceName="PatientInfo
7      <rollingFlatFile rollSizeKB="2024" maxArchivedF
8      <categorySources>
```

4. Edit the following `rollingFlatFile` settings to configure the Event Viewer log files as desired:
   - To change the allowed file size, edit the `rollSizeKB` value
   - To change the allowed number of files, edit the `maxArchivedFiles` value
5. Save and close the *web.config* file.

Picis (web) Services Diagnostics Logging Capabilities

Log Picis (web) Services SQL Queries

To troubleshoot potential issues with the Picis (web) Services, a log file can be enabled to trace the SQL queries that the Picis (web) Services send 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, SQL query logging is disabled. If SQL query logging is enabled, it should be disabled again after troubleshooting is complete (the logs can also be cleared from the Event Viewer).

Enabling SQL query logs

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. Under the `<appSettings>` section, configure the `LogSqlQueries` value as follows:

   ```
   <add key="LogSqlQueries" value="true"/>
   ```
4. Save and close the *web.config* file.
5. To access the log, open the Event Viewer and browse to **Window Logs** > **Application**. By default, the SQL query logs are filed at the Information level.

Configuring SQL query logging category

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. Under the `<appSettings>` section, configure `LogSqlQueriesCategory` to use one of the following values:

   ```
   Debug
   Information
   ```
4. Save and close the *web.config* file.

Disabling SQL query logs

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. Under the `<appSettings>` section, configure the `LogSqlQueries` value as follows:

   ```
   <add key="LogSqlQueries" value="false"/>
   ```
4. Save and close the *web.config* file.

Log Picis (web) Services Request Responses

To troubleshoot potential issues with the Picis (web) Services, a log file can be enabled to trace each time Picis (web) Services responds to a received request. 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 logs can also be cleared from the Event Viewer).

This log that is created includes the following sections:

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

Enabling request response logs

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. Under the `<appSettings>` section, configure the `ProfileServiceCalls` value as follows:

   ```
   <add key="ProfileServiceCalls" value="true"/>
   ```
4. Save and close the *web.config* file.
5. To access the log file, open the Event Viewer and browse to **Window Logs** > **Application**. By default, the request response logs are filed at the Information level.

Disabling request response logs

1. Browse to the folder “C:\inetpub\wwwroot\” and open the folder for the Picis (web) Services logging you want to edit.
2. Open the *web.config* file using a text editor.
3. Under the `<appSettings>` section, configure the `ProfileServiceCalls` value as follows:

   ```
   <add key="ProfileServiceCalls" value="false"/>
   ```
4. Save and close the *web.config* file.

6

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 PCM.NET and is available at the PCM server, and workstations where “clinical module” applications are installed. This tool helps to prevent messages from being lost if they are not received successfully. Message status is displayed so you have visibility on whether or not a message is successfully received by the external systems. If an error occurs, you have the ability to investigate the issue and resend the message.

The status of outbound HL7 messages, sent via the Connectivity Manager (PCM.NET), can be stored in the “clinical module” database based on a notification from the interface 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 Tool rights.

Messaging Log Configurations

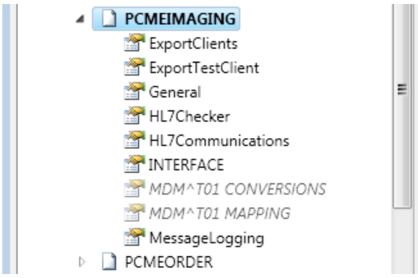
To enable the HL7 Outbound Messaging Log, you must configure both the Messaging Log and each Interface for which you want to log messages.

Configuring an Interface for Message Logging

To enable and Interface for message logging, follow the instructions in the *System Configuration Guide* to add the following settings to the PCME Interface you want to configure. The settings must be added via the Configuration Editor in Customize (PCM>[PCME interface zone]).

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

1. Add a new section named “MessageLogging” to the PCME zone you want to configure to use message logging.

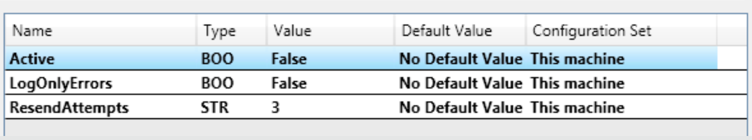


- PCMEIMAGING
  - ExportClients
  - ExportTestClient
  - General
  - HL7Checker
  - HL7Communications
  - INTERFACE
  - MDM^T01 CONVERSIONS
  - MDM^T01 MAPPING
  - MessageLogging
- PCMEORDER

2. Add the following three entries to the new `MessageLogging` section:

Entry Name	Value	Description
`Active`	`True`	Activates the Interface for message logging. True- Messages sent from this PCMHE will be logged in the Message Logging tool. False- Messages sent from this PCMHE will not be logged in the Message Logging tool.
`LogOnlyErrors`	`False`	Force to log only errors. It only applies if parameter Active=True. True- Only messages that failed are logged. False- All messages sent from this PCMHE (either successfully or with errors) will be logged.
`ResendAttempts`	`user-defined`	Limits the number of times the interface tries to resend a message to the HIS. If the parameter is not defined, or its value is lower than or equal to 0, the interface will try to resend the message (if any error) permanently. If the parameter value is greater than 0, the interface will try to resend (if any errors) the number of times defined in the value.

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



Name	Type	Value	Default Value	Configuration Set
Active	BOO	False	No Default Value	This machine
LogOnlyErrors	BOO	False	No Default Value	This machine
ResendAttempts	STR	3	No Default Value	This machine

Note: When configuring multiple Interfaces for message logging, you can copy a section to additional zones, rather than manually creating a new section for each Interface. You can also export sections for later use. For more information on using the Configuration Editor in Customize, see the *System Configuration Guide*.

Configuring the HL7 Outbound Messaging Log

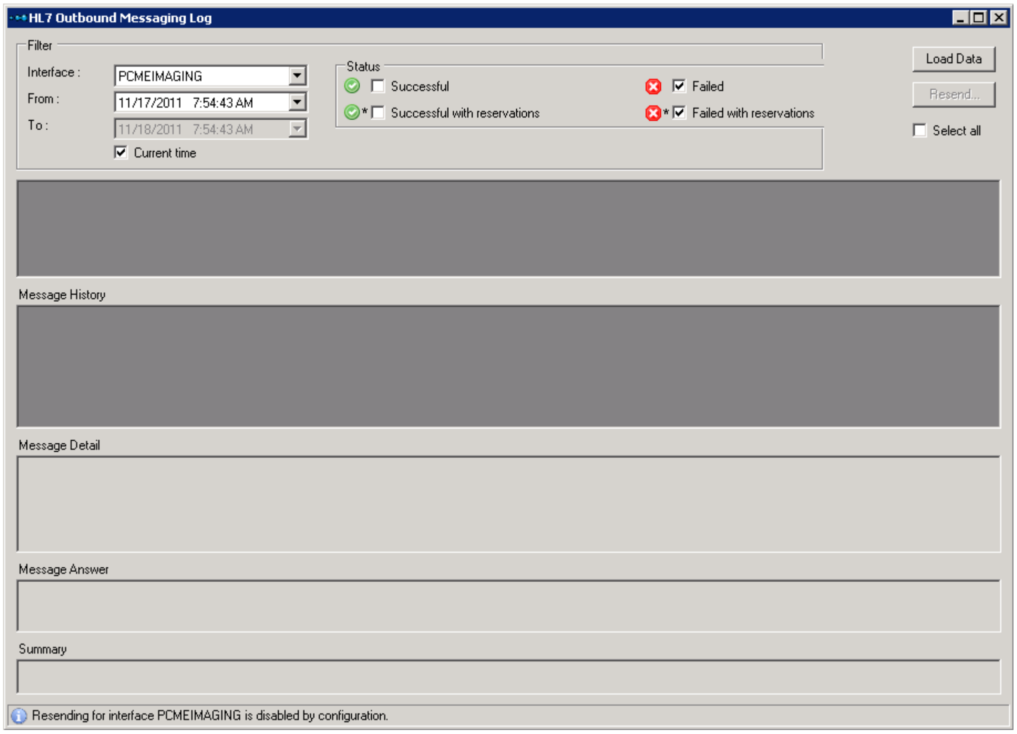
The following entries are configured via the Configuration Editor in Customize. Navigate to PCM > HL7OutputMessagingLog > General and configure these settings as desired.

Setting	Description
DEFAULT_INTERFACE	When the Messaging Log is opened, the Interface filter is set to this value by default.
INTERFACE_LIST	When the Messaging Log is opened, the Interface filter drop-down menu displays the Interface defined in this value.
SENDMESSAGETIMEOUT	Time, in milliseconds, the Interface should wait for any ACK message from PCM.
INTERFACEPLLINHFREQ	Frequency, in milliseconds, to check if current PCM Interface is available or not.

Load Interface Outbound Message Log Data

The Messaging Log displays outbound message data based on filters, which define the types of messages to be returned. There are default filter settings, but you can also edit the filters to narrow or broaden the returned messages.

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



Interface : PCMEIMAGING
From : 11/17/2011 7:54:43 AM
To : 11/18/2011 7:54:43 AM
☑ Current time

□ Successful
□ Successful with reservations
☑ Failed
☑ Failed with reservations

Resending for interface PCMEIMAGING is disabled by configuration.

Viewing Outbound Message Log Data

1. Browse to one of the following locations and double-click the file *HL7OutputMessagingLog.exe* to open the Messaging Log:

   Server: “C:\Picis\Diagnostics”
   Workstation: “C:\Picis\Program Files\Bin”

2. Type your User Name and Password login credentials and click **OK**.

   The HL7 Outbound Messaging Log appears.

3. Click the Interface box and choose the Interface for which you want to view outbound messages.

   > **Note:** The Messaging Log tool can be configured to default to a specific Interface. For more information, see *Configuring the HL7 Outbound Messaging Log* on the previous page.

4. (optional) Click to select the date and status filters to further define the outbound messages you want to load.

   For more information on these filters, see *Filter Outbound Message Log Results* on page 78.

5. Click the **Load Data** button.

   The messages appear in the main grid section, based on your filters.

   The messages are organized based on when they were sent; the latest message status appears on top, and all messages related to a particular patient are visible. When a message is selected in the Main Grid, the Message History, Message Detail, and Message Answer sections are populated.

For more information on these sections, see *Review Outbound Message Log Results* below.

Note: If any of the filtered data changes, a message appears saying that the data displayed does not correspond to the current filter. To apply the new filter, click **Load Data**.

Review Outbound Message Log Results

The messaging log is loaded into a section called Main Grid, directly below the Filters section. Subsequent sections provide more detail about the message and its status.

Main Grid

The Main Grid displays messages that meet the filter criteria. The following columns display information associated with each message in the Main Grid:

- Status- status of the of the outbound message (for details on message statuses see *Message Status Filter* on page 79).
- Error- description of the message error (see *Supported Message Errors* on page 82).
- Extended Error- description of the message error details (see *Supported Message Errors* on page 82).
- Message- the message that was sent.
- Message Time- date and time when the message was sent for the last time (milliseconds resolution).
- Patient ID- unique patient identifier (PTID1).
- Patient Name- Format: based on setting in Configuration Editor DBAPI > DBAPI > Formats > PatientName.
- User Name- full name of the user who sent the message the last time. If the PCMHE interface sent the message, it will be "PCM." Format: based on based on setting in Configuration Editor DBAPI > DBAPI > Formats > PatientName.

Message History Grid

When a message is selected in the Main Grid 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 statuses.

Status	Description
✓	Successful: message sent successfully.
✗	Failed: message send failed.

After the Status, the following columns display information associated with the message in the Message History grid:

- Error- description of the message error (see *Supported Message Errors* on page 82).
- Extended Error- description of the message error details (see *Supported Message Errors* on page 82).
- Message Time- date and time when the message was sent (milliseconds resolution).
- ACK Reception Time- date and time when the Acknowledge Message was received (milliseconds resolution).
- User Name- the full name of the user who sent the message. If the PCMHE Interface sent the message, it will be "PCM." The format is based on based on based on setting in Configuration Editor DBAPI > DBAPI > Formats > PatientName

Message Detail and Message Answer

The Message Detail section displays the entire HL7 message for row that is currently selected in the Message History grid. If an ACK message exists for the selected outbound message, it appears under the Message Answer section.

Summary

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

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

Sent messages are displayed based on which Interface is selected. Each time a new Interface is selected, data is loaded in the grids related to that specific Interface.

The Interface drop-down menu includes the list of PCME 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 74.

Time Range Filter

Messages are displayed based on the time rage that is specified. By default, the "From" time is set minus 24 hours from the current time. You can change this as needed. Message are retrieved based on the current time as the “To” time. To narrow the filter, deselect the Current time box and specify a new “To” time.

Message Status Filter

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

Status	Description
✔	Successful: messages sent successfully.
✖	Failed: every time the message was sent the communication process failed.
✔*	Successful with reservations: the last time the message was sent it succeeded, but other tries in its history failed.
✖*	Failed with reservations: the last time the message was sent it failed, but other tries in its history succeeded.

By default, this filter is set to "Failed" and "Failed with reservations," so only messages with some error appear.

Note: The displayed data automatically updates after Status checkboxes are selected or deselected.

Resend Failed Outbound Messages

PCM Export Interfaces that are configured for message logging can resend messages automatically or you can resend them manually.

Configuring an Interface for Resend Attempts

To define which Interface(s) should allow resend attempts, the following entry should be added in DB Editor’s Configuration Parameters auxiliary table.

CFGVALUEDBOID	3100000000000480000000

CFGVALUE	`NULL`
CFGVALUEDESC	`'PCM HL7 out Remoting endpoint'`
ISDELETED	`'F'`

This setting contains list of endpoint settings. The Messaging Log only resends messages for the PCMHE Interfaces defined in the endpoint list. An endpoint setting parameter is defined as:

```
<PCMEInterface>@@FIELD@@<IP or host name>@@FIELD@@<PORT>
```

where:

`<PCMEInterface>` = the name of the PCM HL7 Export interface.

`<IP or host name>` = TCP/IP or host name where the PCM interface is hosted.

`<PORT>` = endpoint TCP/IP port.

To configure more than one Interface, each configuration must be separated by:

```
@@INTERFACE@@
```

Example:

```
PCMEIMAGING@@FIELD@@192.168.1.5@@FIELD@@1111@@INTERFACE@@PCMEADT
@@FIELD@@192.168.1.6@@FIELD@@4321
```

Automatically Resend Failed Messages

- Configure the `ResendAttempts` configuration setting. For more information, see *Configuring an Interface for Message Logging* on page 74.

  When a message is successfully resent, an acknowledgment is received and the resend attempts cease.

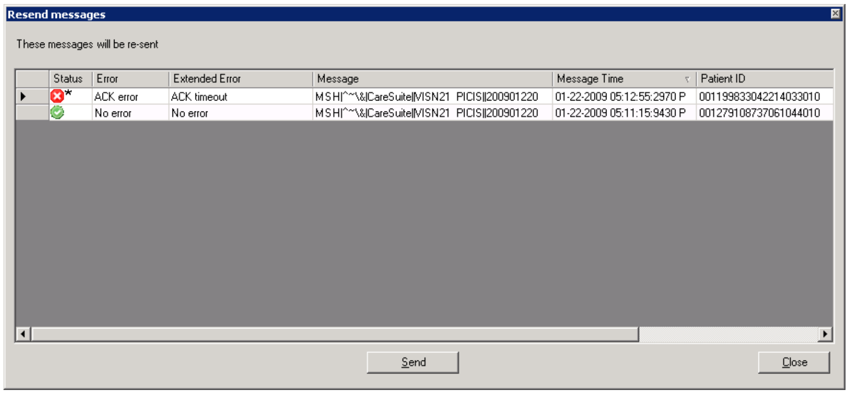
Manually Resend Failed Messages

1. In the Main Grid, click to select the message(s) you want to resend.

   To resend all of the messages, click the **Select All** checkbox (under the Load Data button).

2. Click the **Resend** button.

   If the selected Interface is configured to allow resending messages from the application, after the messages are selected, the Resend Messages confirmation window appears.



These messages will be re-sent

<table>
<tr><th></th><th>Status</th><th>Error</th><th>Extended Error</th><th>Message</th><th>Message Time</th><th>Patient ID</th></tr>
<tr><td>▶</td><td>☒*</td><td>ACK error</td><td>ACK timeout</td><td>MSH|^~\&|CareSuite|MSN21 PICIS||200901220</td><td>01-22-2009 05:12:55:2970 P</td><td>0011998330422140330010</td></tr>
<tr><td></td><td>✓</td><td>No error</td><td>No error</td><td>MSH|^~\&|CareSuite|MSN21 PICIS||200901220</td><td>01-22-2009 05:11:15:9430 P</td><td>0012791087370610440010</td></tr>
</table>

3. Click **Send** to resend the messages.

   When the application attempts to resend messages, they are sent to the PCM Interface and to the HIS simultaneously. When a message is resent its Status icon, Error, and Error Details columns are updated in the main grid.

   The following icons display the status of the message:

Status	Description
⏰	While the message is being sent.
⚠	The message was not delivered to PCM or the operation timed out (the timeout is a configuration parameter).
✓	The message was sent successfully.
☒	The message was sent with errors.

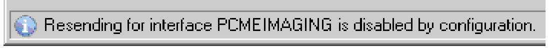
Cancelling a Resend in Process

- Click the **Cancel** button while the process is taking place.

  Messages sent before the cancel action cannot be undone; if PCM has received them, they will be re-sent.

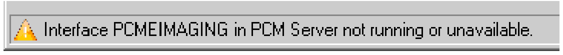
Troubleshooting the HL7 Outbound Messaging Log

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



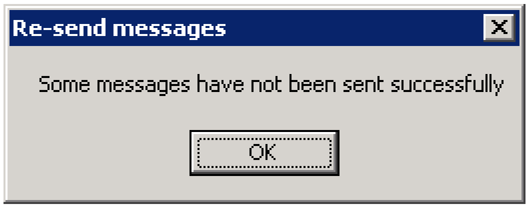
Resending for interface PCMEIMAGING is disabled by configuration.

If the PCM Interface is not configured to allow resending messages, this message will be displayed in the Status Bar.



Interface PCMEIMAGING in PCM Server not running or unavailable.

In the event that the PCM Interface is not available, this message will be displayed in the Status Bar.



Re-send messages

Some messages have not been sent successfully

If the connection with PCM server is broken, this message will be displayed, and the messages not processed after the disconnection will not be sent to the PCM Interface.

Supported Message Errors

The following are message errors supported by the PCM service. Any other possible errors will be logged as "Unknown."

- No Error (0) - No errors occurred during communication.
- AckNotNeeded (14) - the HIS did not send an ACK message and the PCM Interface is configured not to wait for an ACK message from the HIS.
- Nack Errors (1) - the PCMHE Interface received a negative ACK (NACK).
- NackError (1) - the system sent a negative ACK, which specifies an application-level error (e.g.: “Data already processed”).
- NackRejected (2) - the system sent a negative ACK, which specifies that the outer system has rejected the entire message.
- Ack Errors (2) - the PCMHE Interface received a positive ACK with some error.
- AckCustomNoMatch (3) - the PCMHE Interface has a custom ACK message set in the configuration file and the received ACK message does not match the configuration.

  The custom ACK message configuration parameter can be edited via Configuration Editor in Customize (PCM > [PCMHE Interface name] > HL7Communications > HL7HexadecimalCustomAcknowledge).

  This parameter is deactivated by default; users should only activate if needed.
- AckTimedOut (4) - the PCMHE Interface did not receive the ACK message in the expected time.

  Each PCMHE Interface has its own acknowledge timeout, which can be edited via Configuration Editor in Customize (PCM > [PCMHE Interface name] > HL7Communications > AcknowledgeTimeOut).
- AckInvalidFormat (5) - the acknowledge message sent by the outer system is not well formed.
- AckInvalidID (6) - the acknowledge message ID does not match the ID of the message sent by the PCMHE Interface.

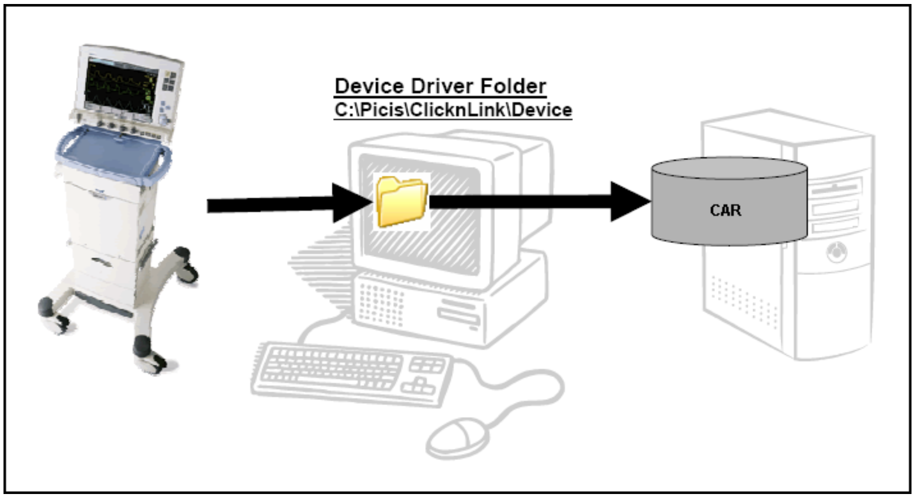
- Comms (3) - A TCPIP error occurred during the communication.
- CommsAbortedConnection (7) - the error can occur when the local network system aborts a connection.
- CommsConnectionBroken (8) - the connection was unexpectedly broken.
- CommsCouldNotCreateSocket (9) - the socket could not be created to establish the connection.
- CommsUnknownHost (10) - the host that the PCMHE Interface is trying to connect is unknown. The name used is not an official hostname or alias.
- CommsCouldNotConnect (11) - could not establish a connection to the outer system.
- Unknown Error (4) - some other errors not typified by the PCM infrastructure.

7 Device Connectivity

Device Connectivity Overview

This chapter presents information for connecting medical devices to bedside workstations with Anesthesia Manager, PACU Manager, or Critical Care Manager installed.

Anesthesia Manager, PACU Manager, and Critical Care Manager collect device data from medical devices connected to the patient.



Workstations with Perioperative and Critical Care applications installed are connected to medical devices via a serial 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 from the medical device and placing it in the CAR database for Anesthesia Manager, PACU Manager, or Critical Care Manager to display at the workstation.

Note: Some device drivers allow connectivity using HL7 (and not serial connection), ask your Picis implementation representative for further information

The following table shows the steps required to install and configure device data.

Action	Explanation
Driver Development	Picis will continue to develop drivers free-of-charge for monitors, ventilators, anesthesia devices, infusion pumps etc., produced by major electromedical device manufacturers including Alaris, Baxter, Braun, GE / Datex, Dräger, Fresenius, Philips, Maquet and Space Labs, in the case where the devices continue to be supported by the manufacturer and comply with Picis RS-232 protocol communication requirements. Driver requests for other less common electromedical devices may be subject to a fee that will be issued by Picis upon receipt of the formal driver request. (Requests can be made via https://users.picis.com). New and updated driver are published at https://users.picis.com. You should review the list and periodically visit the site for updated versions of your drivers. You may also use this site to request a new driver.
Driver Installation	Download the correct driver from https://users.picis.com and install the driver on the workstation. You should note any special instructions in the help file. See *Device Drivers* on page 92 for further information.
Testing the Installation	Testing the installation involves using diagnostic tools to test the installation is correct. See *Troubleshooting Device Drivers* on page 94 for further information.
Configuring Picis applications	Your Clinical Analyst will be responsible for configuring the application to display device data. See the *System Configuration Guide* for further information.
Troubleshooting	During the implementation or as part of ongoing usage you may need to troubleshoot the device driver See *Troubleshooting Device Drivers* on page 94 for further information.

Medical Device Implementations

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

Recommendations

Color Coding System

Establish a color coding scheme for all connections and medical devices:

- Set up a color for each type of medical device to be connected to Perioperative and Critical Care workstations. For example, one color for ventilators and a different color 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-blind users.
- Document the colors and place signs close to the workstations or devices.

Note: A color coding system can not be used with serial expanders.

Cable and Connections

General improvement for connections/cables:

- Tie loose cables together to avoid long, loose and untidy cabling.
- Use high quality connectors/protection connectors.
- Ensure replacement cables and connectors are available in case of failure.

Mobile Arms

If you are using a mobile arm install it with cabling included:

- Set up all cabling fixed inside mobile arms
- Use ports in walls/mobile arms for final connection to medical device.

Serial Expander Connections

Review serial expander connections to computers:

- Fix connections to prevent movement and/or disconnections.
- Ensure cables are created to serial expander pinout specifications. These are specific to the manufacturer and not provided by Picis. All specifications provided by Picis are for connecting directly to a workstation.

Testing and Upgrading

Allow adequate time to test new drivers and firmware, noting that updated versions of the drivers will be sent to you, by Picis, 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 (com) settings, RS-232 incorrectly configured, installed incorrectly or connected to the wrong communications (com) port).
- Cables inadequately connected (stepping on cables, broken connectors, incorrect connectors for devices or loose connections).
- Serial expander poorly connected.
- Serial expander incorrectly configured.
- Wrong cable used for a specific device.
- Cables connectors break due to a tight connection.
- The medical device does not support serial communication. An extra setting needs configuring by the device manufacturer.
- Devices connected with incorrect device driver loaded by the Perioperative and Critical Care applications.

Practical Examples

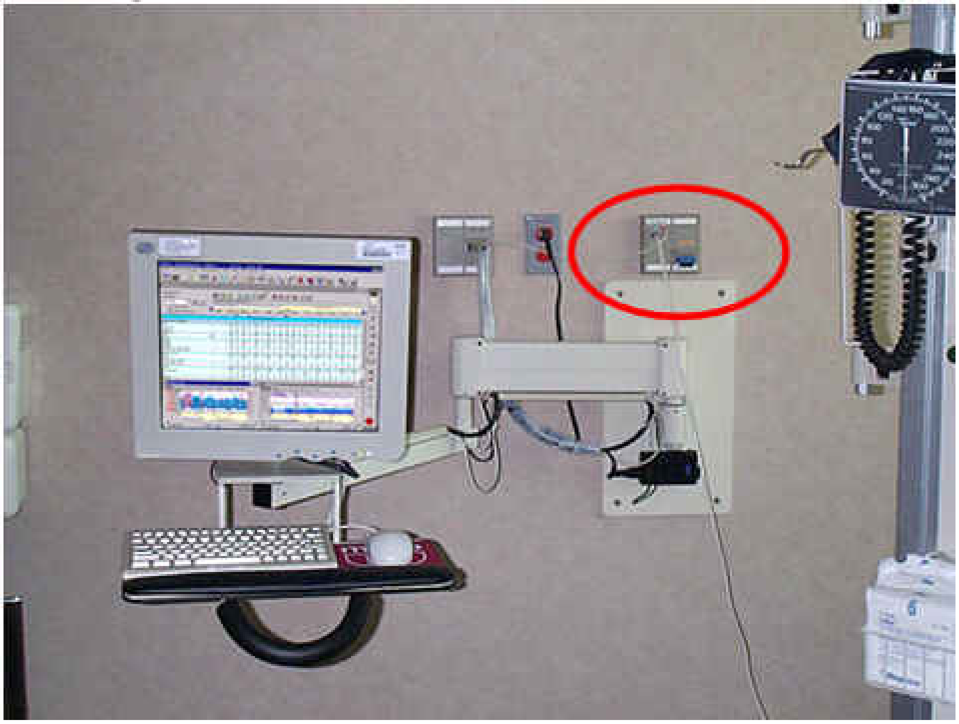
The following pictures show some example configurations of medical devices.

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

The circles highlights the specific details.

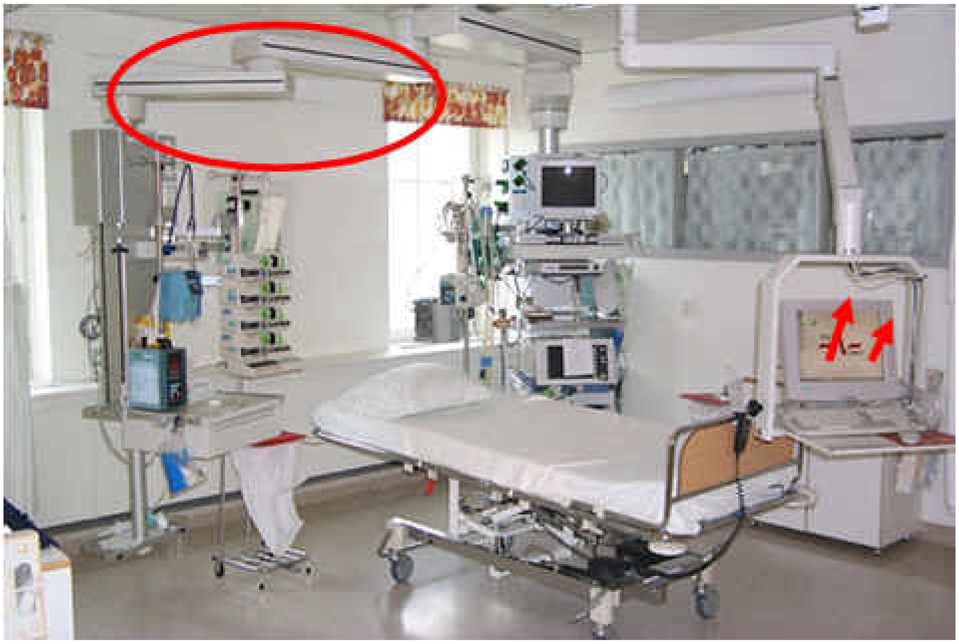
Mobile Arm with hidden computer

The mobile arm protects and hides the cables. The computer is positioned behind the wall.



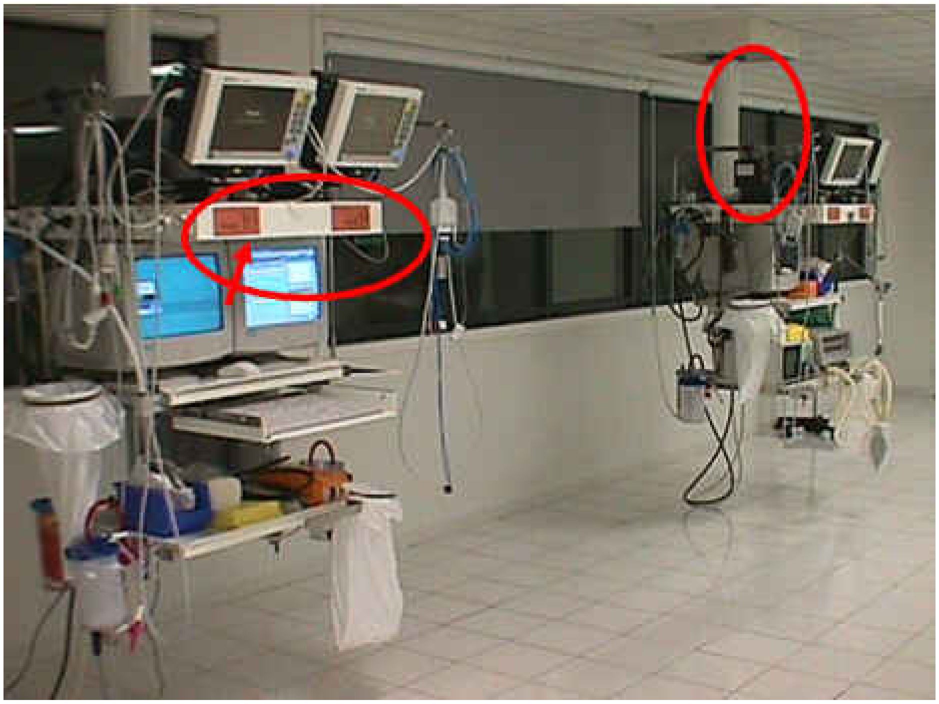
Mobile arms with cables protected

The mobile arm protects and hides the cables. The computer is positioned behind the wall



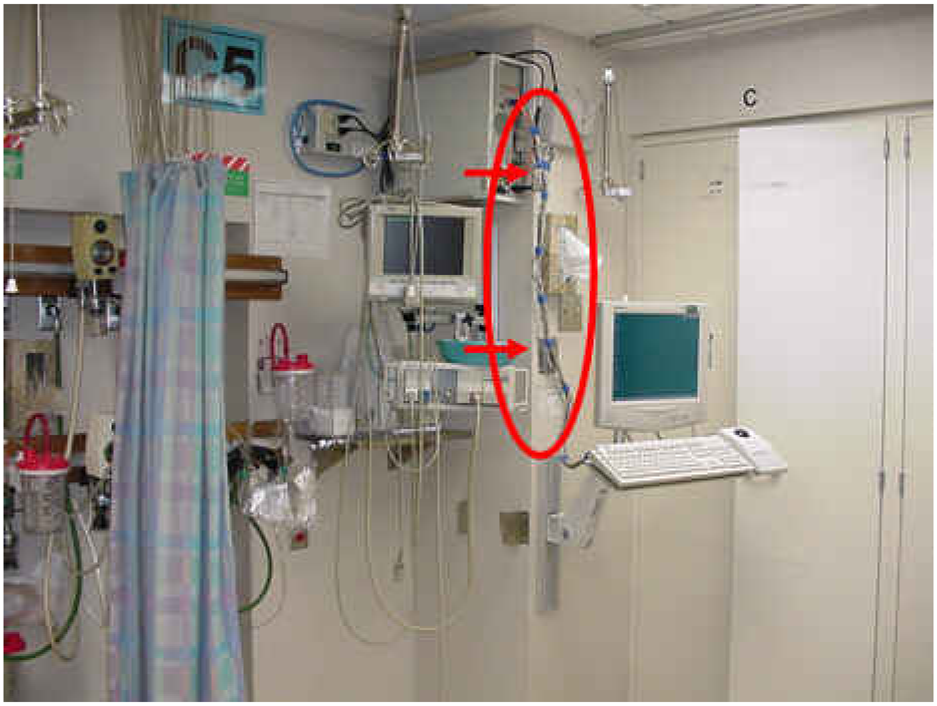
Standard Configuration for mobile devices.

Units are configured with standard ports and devices so mobile devices can be attached.



Organizing Cables

Cables are fastened to avoid interfering with patient care.



Device Drivers

Device drivers are developed using two complimentary technologies. The following table shows the difference between these methods:

Attribute	Click'n Link	New Kernel Technology (NKT)
Architecture	Uses its own API	Interfaces directly with the Kernel.
Devices Supported	Electromedical devices for example Monitors, Ventilators and Anesthesia Devices	Electromedical devices for example Monitors, ventilators and Anesthesia Devices. Infusion Pumps with fluids.
Diagnostic Tool	Click'n Link Spy	NKT Spy

Attribute	Click’n Link	New Kernel Technology (NKT)
Driver Identification	Click’n Link device driver files begin with a 5.x (for example V5500).	NKT device driver files begin with a 8.y (for example V8.0.0.1).

Device Driver Contents

Device drivers are downloaded from the users website as Zip files they contain the following files:

File	Description
DLL	The binary code which interprets the data received from the medical device.
Help File (hlp or chm)	Help file which explains the cabling specifications, device variables and any special usage instructions.
Configuration Files	Some drivers require one or more of these files to determine variable or communication settings: (filename.00x) - Universal Drivers (filename.ini) - Cobe HLM, Marquette Unity, Siemens Infinity, etc. (filename.cfg) - SpaceLabs PC
ReadMe.txt file	This file contains a short description of the changes introduced in each driver version.

Requesting a device driver

Drivers for medical devices are available on request from the Picis Help Desk.

Installing a device on a workstation

1. Double-click the device driver zip file.
2. Extract the file to “<Picis installation folder>\ClicknLink\Device.”

Note: Some drivers required additional installations steps. These will be contained in driver Zip file.

Testing a device driver using Click’n Link Spy

Note: Click’n Link device drivers number start with a 5.x.

1. Close Anesthesia Manager, PACU Manager, or Critical Care Manager.
2. Browse to the “C:\Program Files (x86)\Picis\Bin” folder and double-click the file **CnlSpy.exe**.

> **Note:** You will need the Diagnostics Tools system right to open Click ´n Link Spy. See your Picis system administrator if you are not able to open Click ´n Link Spy.

3. From under **Device Driver,** select a driver you want to load.
4. Under **Serial Port**, select the serial port to which the device is connected.
5. Click **Start**.
6. Click **Stop** to end the session.

Testing a driver using NKT Spy

> **Note:** NKT device drivers number start with a 8.y.

1. Close Anesthesia Manager, PACU Manager, or Critical Care Manager.
2. Browse to the “C:\Program Files (x86)\Picis\Bin” folder and double-click the file *NKTSpy.exe*.

> **Note:** You will need the Diagnostics Tools system right to open NKT Spy. Contact your system administrator if you are not able to open NKT Spy.

3. From under **Driver**, select a driver you want to load.
4. Under **Port**, select the serial port to which the device is connected.
5. Click **Start**.
6. Click **Stop** to end the session.

Interpreting Device Driver Diagnostic Tools

Both diagnostics tools record raw data and decoded data. Raw data is displayed in the format that is received from the device whereas decoded data is seen as it will be displayed in the application.

Troubleshooting Device Drivers

Device driver troubleshooting is divided into two areas:

- **Hardware**: Physical connection problems exists between the workstation and medical device driver. In the diagnostics tools no data will be visible in the Raw Data window. See *Potential Hardware Issues* on page 88 for a list of possible causes.
- **Software Driver**: There might be an issue with the device driver used. The following are possible causes:
  - Wrong version of the driver might being used. See *Requesting a device driver* on the previous page for information about downloading the latest version of a driver.

- Software upgraded on medical devices but incompatible with Perioperative and Critical Care software. Contact your Picis representative for more information.
- Device driver is incorrectly recording data. Contact Picis support who may ask you to create a log file. See *Creating a log file using Click'n Link Spy* below and *Creating a log file using NKT Spy* below for further details.

Creating a log file using Click'n Link Spy

> **Note:** The latest drivers now create automatic logs files in the format <ComputerName>_ <DriverName>mmddyyyy. These daily log files are created in the same folder as the DLL. The are deleted when they are two days old.

1. Close Anesthesia Manager, PACU Manager or Critical Care Manager.
2. Browse to “C:\Program Files (x86)\Picis\Bin” and double-click the file *CnlSpy.exe.*

   > **Note:** You will need the Diagnostics Tools system right to open Click ´n Link Spy. See your Picis system administrator if you are not able to open Click ´n Link Spy.

3. From under **Device Driver,** select a driver you want to troubleshoot.
4. Under **Serial Port**, select the serial port to which the device is connected.
5. Click **More** and next to **Output File**, enter path and filename for the file you want to create.
6. Click **OK** when you have finished.
7. Click **Start**.
8. Click **Stop** to end the session.

Creating a log file using NKT Spy

1. Close Anesthesia Manager, PACU Manager or Critical Care Manager.
2. Browse to “C:\Program Files (x86)\Picis\Bin” and open the file *NKTSpy.exe*.

   > **Note:** You will need the Diagnostics Tools system right to open NKT Spy. See your Picis system administrator if you are not able to open NKT Spy.

3. From under **Driver,** select a driver you want to troubleshoot.
4. Under **Port**, select the serial port to which the device is connected.
5. Next to **Output File**, enter path and filename for the file you want to create.
6. Click **Start**.
7. Click **Stop** to end the session.

Viewing a log file using Click'n Link Spy

1. Close Anesthesia Manager, PACU Manager or Critical Care Manager.
2. Browse to “C:\Program Files (x86)\Picis\Bin” and open the file *CnlSpy.exe*.

> **Note:** You will need the Diagnostics Tools system right to open Click ´n Link Spy. See your Picis system administrator if you are not able to open Click ´n Link Spy.

3. From under **Device Driver**, select the driver you want to view.
4. Click **More** and next to **Source File**, enter path and filename of file to be viewed.
5. Click **OK** when you have finished.
6. Click **Start**.
7. Use the arrow keys at the bottom of the screen to navigate through data collection points.

Viewing a log file using NKT Spy

1. Close Anesthesia Manager, PACU Manager or Critical Care Manager.
2. Browse to “C:\Program Files (x86)\Picis\Bin” and open the file *NKTSpy.exe*.

> **Note:** You will need the Diagnostics Tools system right to open NKT Spy. See your Picis system administrator if you are not able to open NKT Spy.

3. From under **Driver**, select a driver you want to troubleshoot.
4. Next to **Source File**, enter path and filename for the file you want to view.
5. Click **Start**.
6. Use the arrow keys at the bottom of the screen to navigate through data collection points.

Perfect Trace and NKT Drivers

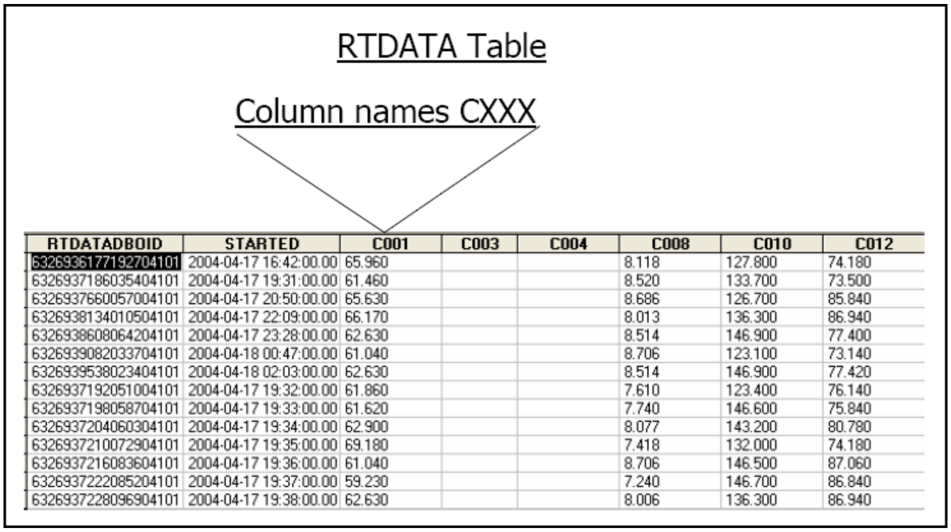
Perfect Trace can be used to log NKT drivers. Perfect Trace stores the same information as NKT Spy and additionally application messages. Perfect Trace is used when troubleshooting problems related to application activity not just the device driver. See *Perfect Trace* on page 56 for more information.

Device Data Stored in the Database

Device data is stored in the database in three tables:

- *RTDATA* - Stores device data.
- *RTDATAVALIDATED* - Stores device data that is validated.
- *RTDATAAUDITED* - Stores device data that is audited or edited.

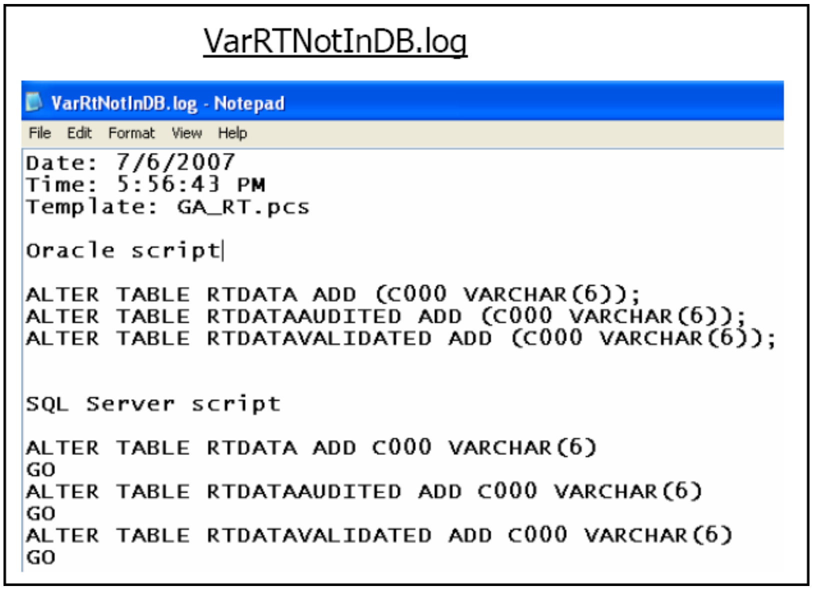
To optimize database storage in these tables each column represents a different variable. The title of the column is Click’n Link code (CXXX) for the variable. (For full list of codes and variables see the Physiologic Variables table in DB Editor).



RTDATADBOID	STARTED	C001	C003	C004	C008	C010	C012
6326936177192704101	2004-04-17 16:42:00.00	65.960			8.118	127.800	74.180
6326937186035404101	2004-04-17 19:31:00.00	61.460			8.520	133.700	73.500
6326937660057004101	2004-04-17 20:50:00.00	65.630			8.686	126.700	85.840
6326938134010504101	2004-04-17 22:09:00.00	66.170			8.013	136.300	86.940
6326938608064204101	2004-04-17 23:28:00.00	62.630			8.514	146.900	77.400
6326939082033704101	2004-04-18 00:47:00.00	61.040			8.706	123.100	73.140
6326939538023404101	2004-04-18 02:03:00.00	62.630			8.514	146.900	77.420
6326937192051004101	2004-04-17 19:32:00.00	61.860			7.610	123.400	76.140
6326937198058704101	2004-04-17 19:33:00.00	61.620			7.740	146.600	75.840
6326937204060304101	2004-04-17 19:34:00.00	62.900			8.077	143.200	80.780
6326937210072904101	2004-04-17 19:35:00.00	69.180			7.418	132.000	74.180
6326937216083604101	2004-04-17 19:36:00.00	61.040			8.706	146.500	87.060
6326937222085204101	2004-04-17 19:37:00.00	59.230			7.240	146.700	86.840
6326937228096904101	2004-04-17 19:38:00.00	62.630			8.006	136.300	86.940

In each database these tables will be slightly different based on the device drivers installed. Also, if a new device is installed, more Click'n Link variables may be added and a corresponding column will need to be created in the database.

The typical workflow would be that the new device is installed (including the driver), a clinical user will then add the device variables in Customize to one or more templates. As the clinical user saves the configuration they will be warned that there are new database variables to be created. A file named *VARRTNOTINDB.log* with the database statements will be stored in the %PicisCommonAppData" folder ("C:\ProgramData\Picis\<ALIAS>").



```
Date: 7/6/2007
Time: 5:56:43 PM
Template: GA_RT.pcs

Oracle script

ALTER TABLE RTDATA ADD (C000 VARCHAR(6));
ALTER TABLE RTDATAAUDITED ADD (C000 VARCHAR(6));
ALTER TABLE RTDATAVALIDATED ADD (C000 VARCHAR(6));


SQL Server script

ALTER TABLE RTDATA ADD C000 VARCHAR(6)
GO
ALTER TABLE RTDATAAUDITED ADD C000 VARCHAR(6)
GO
ALTER TABLE RTDATAVALIDATED ADD C000 VARCHAR(6)
GO
```

Creating a new database column in the RTDATA tables

This procedure should only be undertaken by a qualified database administrator who has administrator access to the CAR database. If you are in any doubt contact Picis support before proceeding.

1. Open SQL Server Management Studio and select to the CAR database.
2. Copy and paste the contents of *VarRTNotInDB.log*. (You only need copy the version for you database vendor).
3. Review the script to ensure all variables to be created are numeric.
4. Run the script.
5. Run the following script and check the columns have been added to the RTDATA table:

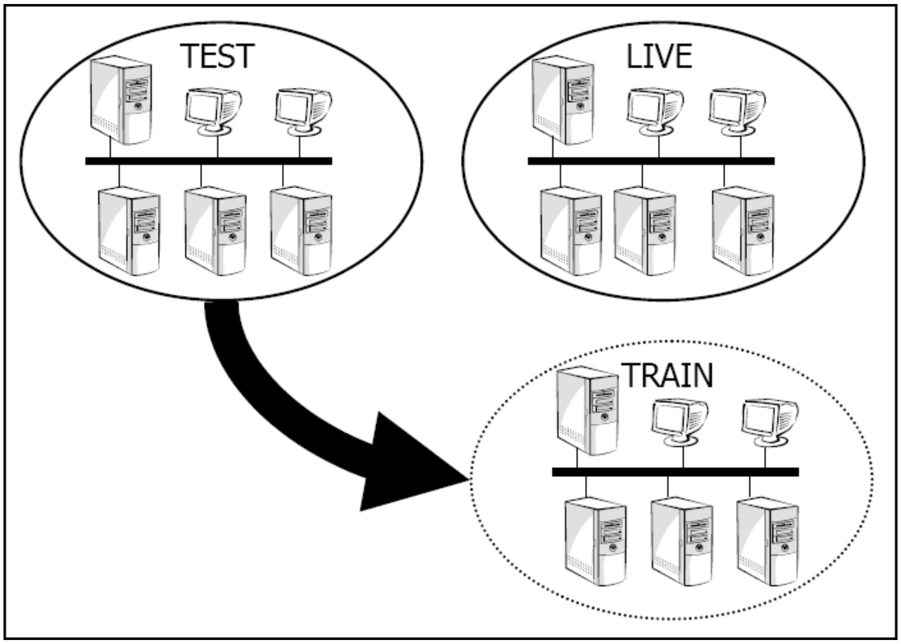
   ```
   Select * RTDATA
   ```

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

8

Additional Environments

Create Additional Environments



If an additional environment is required, for example Train or Build, Picis can advise on the creation, however the installation, upgrade, and support will remain the responsibility of the customer. It is recommended that customers make a copy of their test environments in order to create the additional environments. If the additional environment requires updating it should be recreated by copying test again.

Note: In addition to TEST and LIVE environments, sites that are already live with one product and want to install additional modules to become a TPA system, for example, will need a third environment—DEV. The DEV environment is used for building the integrated TPA system while leaving the TEST environment free for troubleshooting and testing any service packs or minor updates that may be required during the time it takes to implement the TPA system. (The DEV environment is only supported by Picis until the TPA system goes live. Then the DEV environment becomes the new TEST environment and the existing TEST environment is annulled).

Creating Additional Environments

Note: This procedure references other documents which are available from the *User Community site* at *https://users.picis.com.*

1. Prepare and configure the Database server: See the Installation Guides for detailed instructions.
2. Copy the Test Databases: See the procedure *Copying Perioperative and Critical Care system databases* below for further information.
3. Rename the Database: See *Renaming a database in the Perioperative and Critical Care system* on page 104 for further information.
4. Recreate the Users and Logins: See *Recreating the users and logins for Perioperative and Critical Care system databases* on page 105 for further information.
5. Install and Connect the application workstations: See the *Workstation Installation Guide*.
6. Install the background servers; see the *Server Installation Guide*.

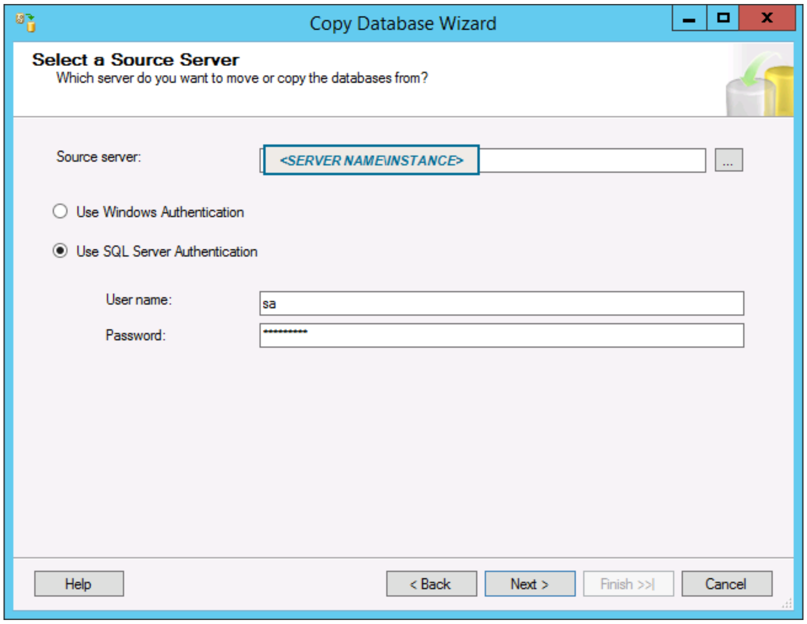
Copying Perioperative and Critical Care system databases

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

1. Before copying a database no user or process should be connected to the database. Additionally, all other servers except the database server should be stopped.
2. At the source the Database Server, click the **Start** button and then point to **Programs**.
3. Point to **Microsoft SQL Server** folder and then click **Management Studio**.
4. In the Connect to Server window, type the server details and the user login credentials.

   Database details appear in SQL Server Management Studio’s Object Explorer.
5. In the Object Explorer, click to expand **Databases**, under the SQL Server instance.
6. Right-click the **Databases** and then click **Tasks** > **Copy Database**.

   The Copy Database Wizard appears.
7. Click **Next**.
   The Select a Source Server window appears.



Select a Source Server
Which server do you want to move or copy the databases from?

Source server: <SERVER NAME\INSTANCE>

○ Use Windows Authentication

● Use SQL Server Authentication

User name: sa

Password: **********

8. In the **Source server** field, type the name of the source server (including the instance name).

   Example: PICISSERVER\TEST

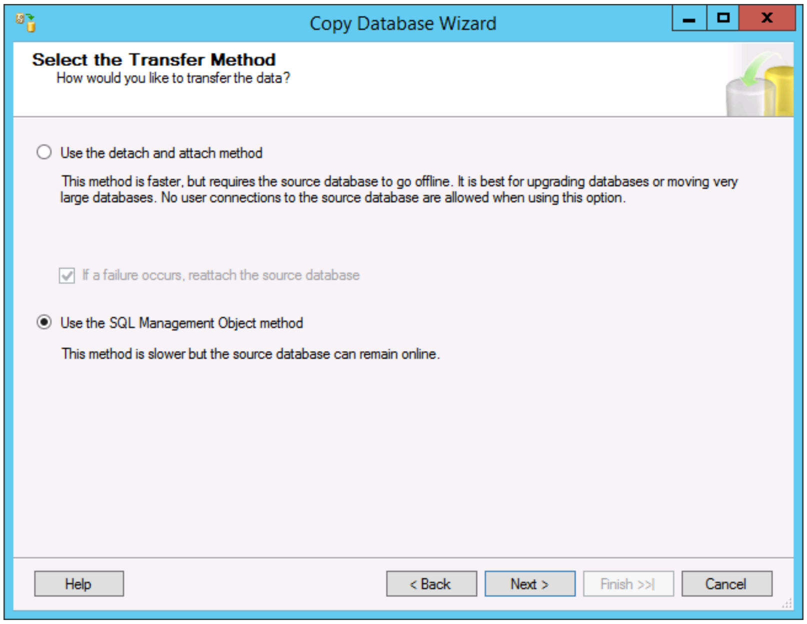
   Note: The SQL instance that you selected in Object Explorer defaults into this field.

9. Select **Use SQL Server Authentication**.
10. In the User name field, type **sa**. (By default this should already be entered).
11. In the **Password** field, type the **sa password**. (By default this should already be entered).
12. Click **Next**.
    The Select a Destination Server window appears.
13. In the Destination server field, type the name of the destination server (including the instance name).

    Example: PICISSERVER2\TRAIN

14. Select **Use SQL Server Authentication**.
15. In the **User name** field, type the **sa**.
16. In the **Password** field, type the sa password and click **Next**.

    The Select the Transfer Method window appears.



Copy Database Wizard

Select the Transfer Method

How would you like to transfer the data?

○ Use the detach and attach method

This method is faster, but requires the source database to go offline. It is best for upgrading databases or moving very large databases. No user connections to the source database are allowed when using this option.

☑ If a failure occurs, reattach the source database

● Use the SQL Management Object method

This method is slower but the source database can remain online.

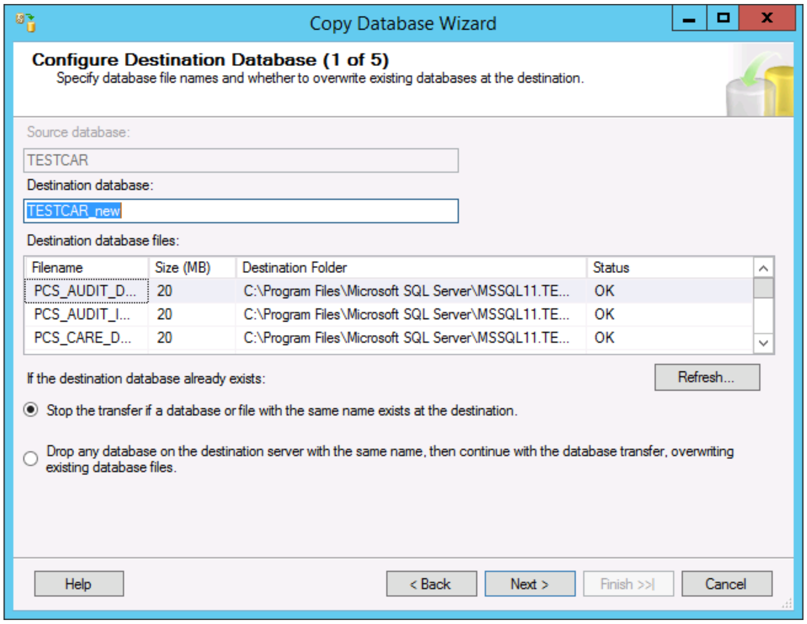
17. Select **Use the SQL Management Object Method** and click **Next**.
    The Select Databases window appears.

18. In the **Copy** column, select the box next to each database in your database set.

    > **Note:** Be sure to select the Copy column and not the Move column.

19. Click **Next** when you have finished.

    The Configure Destination Database window appears.



Copy Database Wizard

Configure Destination Database (1 of 5)
Specify database file names and whether to overwrite existing databases at the destination.

Source database:
TESTCAR
Destination database:
TESTCAR_new
Destination database files:

Filename	Size (MB)	Destination Folder	Status
PCS_AUDIT_D...	20	C:\Program Files\Microsoft SQL Server\MSSQL11.TE...	OK
PCS_AUDIT_I...	20	C:\Program Files\Microsoft SQL Server\MSSQL11.TE...	OK
PCS_CARE_D...	20	C:\Program Files\Microsoft SQL Server\MSSQL11.TE...	OK

If the destination database already exists:

● Stop the transfer if a database or file with the same name exists at the destination.

○ Drop any database on the destination server with the same name, then continue with the database transfer, overwriting existing database files.

20. In the Destination database field, type the name of the destination database.

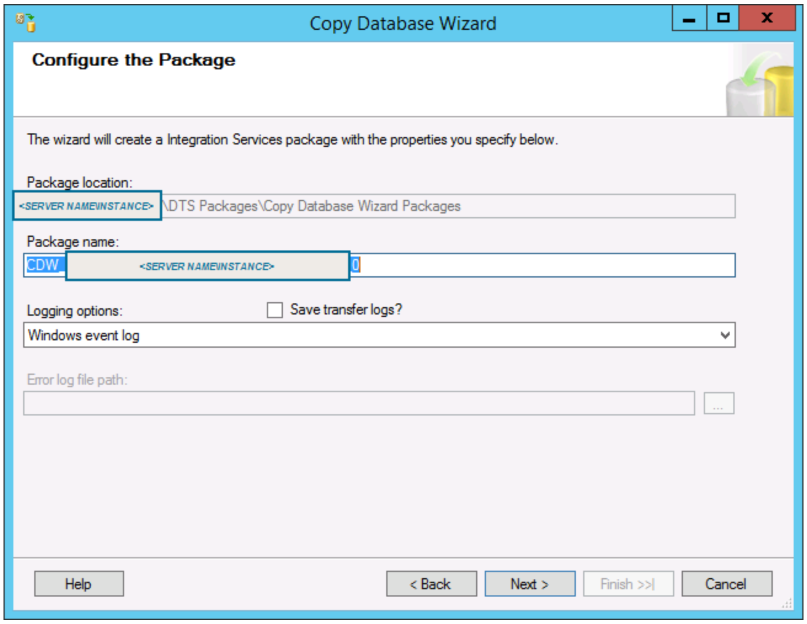
> **Note:** The databases name for most environments (except live) are prefixed with the environment name, so you should be sure to change the prefix to specify the correct environment (“testPSM” to “devPSM” for example).

(optional) In the Filename column, click the file name and type the new name.

(optional) In the Destination Folder column, click the path and type the new path.

21. Click **Next**. If you selected more than one database to copy, the next database appears. Follow the instructions in steps 20, 21, and 22 for each database in turn.
22. After the final database has been configured, click **Next**.

    The Configure the Package window appears.



Configure the Package

The wizard will create a Integration Services package with the properties you specify below.

Package location: <SERVER NAME\INSTANCE>\DTS Packages\Copy Database Wizard Packages

Package name: CDW <SERVER NAME\INSTANCE> 0

Logging options: Windows event log

□ Save transfer logs?

Error log file path:

(optional) Edit the package details, if desired, then click **Next**.

The Schedule the Package window appears.

23. Keep the default settings and click **Next**.

    A summary of your settings appears. Review your entries to ensure they are accurate.

24. Click **Finish** to close the wizard and confirm the copy.

    You may have created the logins on the new server so this may provoke an error during the transfer. This can be safely ignored.

    Each object will be copied. After the copy is complete you should review the Status column to see if there are any red Xs denoting a failed copy of an object. Review the specific object to see if it is a User name issue, which can be ignored, or requires further investigation.

25. Click **Close** to close the window.

Renaming a database in the Perioperative and Critical Care system

This procedure describes how to rename a database.

1. From the Database server, click the **Start** > **Programs** > **Microsoft SQL Server** > **Management Studio**.
2. In the Connect to Server window, type the server details and the user login credentials.
3. Open the script “Non DBUtility Files\Useful SQL*Database Rename.sql*.”
4. Click **F5** to execute the query.
5. Use DB Utility to Confirm DB Pointers and then run all of the relevant post-upgrade scripts to updatge all of the locations where the previous database name is referenced in other databases.

   For information on DB Utility, see Appendix A in the *Server Installation Guide*.

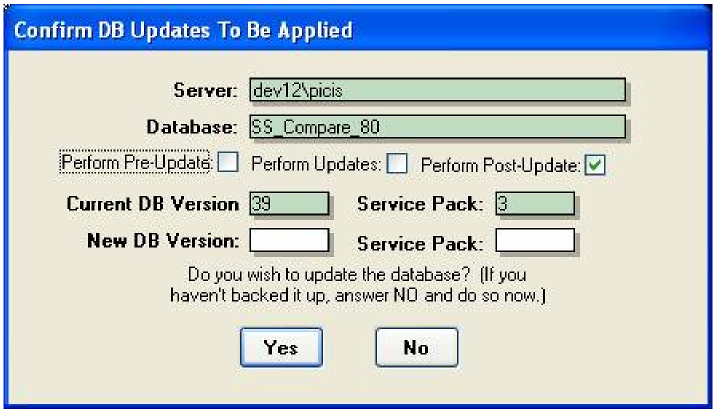
Recreating the users and logins for Perioperative and Critical Care system databases

This procedure describes how to recreate Picis Perioperative and Critical Care database users and should be performed against all copied databases.

DB Utility is needed. For more information on any of the steps, see the Appendix A in the *Server Installation Guide.*

1. Start and configure DB Utility.
2. Retrieve the database set. (If necessary, first create a database set.)
3. Select the database in the bottom pane and click **Update Databases**.

   A window such as the following appears:



Confirm DB Updates To Be Applied

Server: dev12\picis
Database: SS_Compare_80
Perform Pre-Update: □ Perform Updates: □ Perform Post-Update: ☑
Current DB Version 39 Service Pack: 3
New DB Version: Service Pack:

Do you wish to update the database? (If you haven't backed it up, answer NO and do so now.)

4. Select the **Perform Post-Update** check box and leave the other fields blank.
5. Click **Yes**.

   A window will show the scripts that will be run against the database.
6. Click **Proceed with the Update.**The installation will proceed.

   Respond to the question as the subsequent windows appear.
7. Click **OK** when the confirmation window appears.

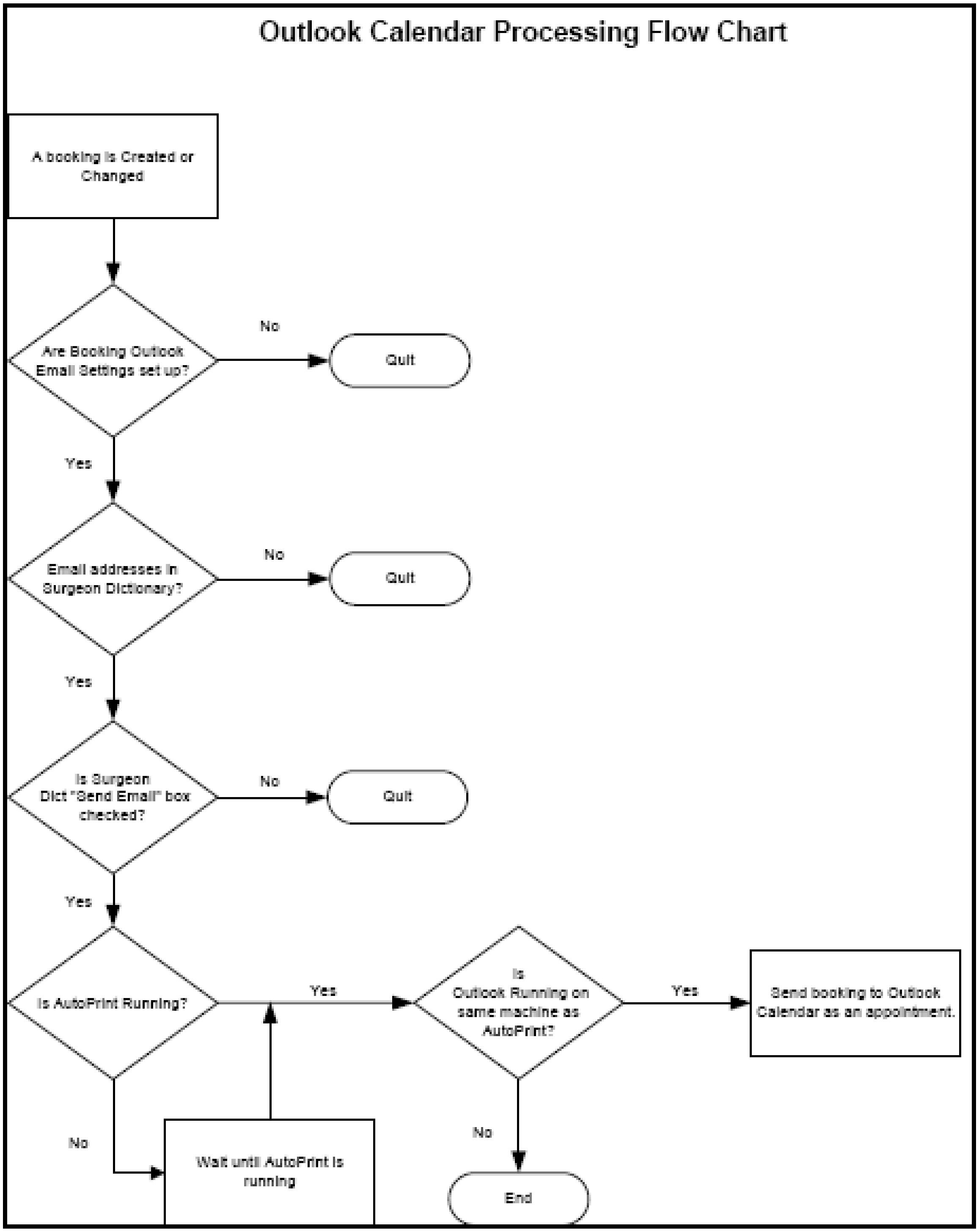
9

Outlook Booking Appointment Settings

Workflow Overview

OR Manager customers who use Microsoft Outlook can use the Booking Outlook Email Settings screen to set up parameters to automatically send new or changed bookings to the Outlook calendars of surgeons and anesthesiologists.

This diagram shows what happens when the OR Manager to Outlook Calendar feature is set up and running:


Outlook Calendar Processing Flow Chart
A booking is Created or Changed
Are Booking Outlook Email Settings set up?
No
Quit
Yes
Email addresses in Surgeon Dictionary?
No
Quit
Yes
Is Surgeon Dict "Send Email" box checked?
No
Quit
Yes
Is AutoPrint Running?
Yes
Is Outlook Running on same machine as AutoPrint?
Yes
Send booking to Outlook Calendar as an appointment.
No
Wait until AutoPrint is running
No
End

Additional Rules for Sending 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 anesthesiologists

Rules for Bookings

The rules related to the booking itself are presented in the order that they are performed in the software:

1. If the **Send Booking Mails** box is not checked, do not send the appointment.
2. If the surgery date is within the number of days in the **Suppress emails _ days before surgery** box when the user creates or changes the booking, do not send the appointment.

   > ***Example:*** If today is Dec 9, 2015 and the suppress email days is set to 2, and the user is changing a booking with a book date of Dec 9, 2015 or Dec 10, 2015, 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 Request or Wait List, do not send an appointment.
5. If it is a new booking, send the appointment.
6. If booking date is modified (future booking date), send appointment, except if the date is within the suppress emails limit.
7. If setup start time or teardown end time is changed then send an appointment.
8. If any new surgeon is added on 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 Canceled, send a Cancel appointment.
3. If a cancelled booking is changed to active, send a New appointment.
4. If a requested or waitlisted 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 Cancel appointment for the old surgeon and a New appointment for the new surgeon. This works for complex as well as simple bookings.

7. If any of the procedures for this surgeon has been changed or swapped with another procedure, send an Update appointment.
8. If any of the procedures for this surgeon has been deleted, send an Updated appointment.
9. If any new procedure is added for this surgeon, send an Updated appointment.
10. If the booking start time or end time has changed, send an Updated appointment.
11. If the booking date has changed, send an Updated appointment.
12. If any existing surgeon is deleted from booking, send Cancel appointment. Before generating the cancel appointment message, the system prefixes cancel reason and cancel comment in the message body.

    Otherwise, do not send an appointment.

    See *Workflow Overview* on page 107 and *Booking Outlook Email Settings* on the facing page to see what happens once it is determined that an appointment should be sent. Additionally:

    - While generating an Update appointment, it checks to see if there was a new or updated appointment already sent for this surgeon or assistants for the booking. If not, it creates a new appointment.
    - While generating Cancel appointments, Autoprint checks if there were any new or updated appointments sent for this surgeon or assistants for this booking. If not, it will not send a cancel appointment, because surgeon has never received an appointment for this booking in the first place.

Rules for Anesthesiologists

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 waitlisted booking is changed to active, send an Update appointment.
5. If a booking start time or end time, as defined in the Booking Outlook Email Settings, has changed, send an Updated appointment.

Calendar Feature Setup

Setting up the OR Manager to Outlook Calendar feature must be done in three different components of your installation:

- OR Manager setup
- Autoprint setup
- Outlook setup

Prerequisites

Before the OR 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. This feature has been certified for use with the supported Microsoft Outlook version 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 Autoprint.

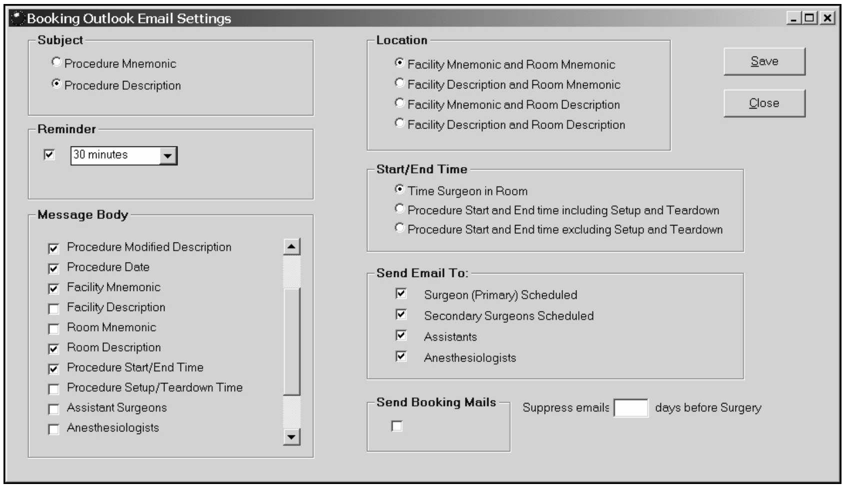
OR Manager Setup

After the prerequisites are met, the follow must be completed in OR Manager:

- The email address information for each surgeon and anesthesiologist whose Outlook calendars are to be made available for bookings must be in the Surgeon dictionary and the **Send 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

OR Manager creates each appointment's subject, location, start and end times, and message body according to how you set up the Booking Outlook Email Settings screen (**Maintenance** > **Bookings** > **Outlook Appointment Settings)**:



Subject
○ Procedure Mnemonic
● Procedure Description

Reminder
☑ 30 minutes

Message Body
☑ Procedure Modified Description
☑ Procedure Date
☑ Facility Mnemonic
☐ Facility Description
☐ Room Mnemonic
☑ Room Description
☑ Procedure Start/End Time
☐ Procedure Setup/Teardown Time
☐ Assistant Surgeons
☐ Anesthesiologists

Location
● Facility Mnemonic and Room Mnemonic
○ Facility Description and Room Mnemonic
○ Facility Mnemonic and Room Description
○ Facility Description and Room Description

Start/End Time
● Time Surgeon in Room
○ Procedure Start and End time including Setup and Teardown
○ Procedure Start and End time excluding Setup and Teardown

Send Email To:
☑ Surgeon (Primary) Scheduled
☑ Secondary Surgeons Scheduled
☑ Assistants
☑ Anesthesiologists

Send Booking Mails
☐

Suppress emails ____ days before Surgery

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

> ***Example:*** Should the subject show the Procedure Mnemonic or the Procedure Description? What information should be in the message body? How should the facility and room display for Location?

2. Select **Reminder** if you want to have Outlook send a reminder before the booking. (Then select the number of minutes, hours, or days before the surgery you want the reminder to be sent.)
3. Select **Send Booking Mails**. This sets the system flag *send_booking_email* to Y to enable booking changes to be sent to Outlook.
4. Enter a number in the **Suppress emails _ days before surgery** box to keep Autoprint from posting Outlook Calendar appointments earlier than the specified number of days before the operation. Leave blank to allow appointments to be posted right up to the day of the operation.

Autoprint Setup

Prerequisites:

- Microsoft Outlook must be installed on the server where Autoprint is installed.
- An empty row should exist in the PSM database's Destinations table. This should have been completed as part of the server installation.

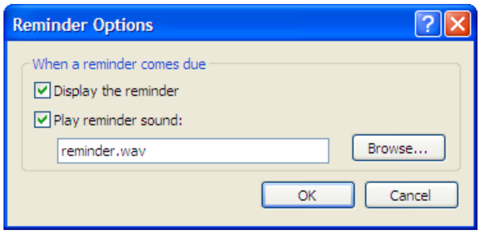
1. Create a new Outlook user profile, *Autoprint*, that can sign into Outlook and send mail. *Autoprint* should appear in your hospital's main address book.
2. Use Autoprint to create an *Autoprint* email entry
   See *Autoprint* on page 38 for further information.

Outlook Setup

1. Create a new Outlook user profile, *Autoprint*, which can sign onto Outlook and send mail.
2. Because OR Manager sends appointments from the Autoprint Server, you won't want to see reminders pop-up on the server. Make sure that you turn off the reminder pop-ups on Autoprint machine through Outlook.

Turning off the reminder pop-ups

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



4. Deselect the **Display the Reminder** checkbox.

   If your site has installed Outlook E-mail security updates (SR-1) this enhancement will need additional setup. See *Outlook SR-1 Background* below.

Outlook SR-1 Background

If you have the SR-1 service pack installed, Outlook displays a warning when the Autoprint application sends an appointment. Because Autoprint has no user who can click on this window, you must make some changes in the settings for the *Autoprint* Outlook user profile.

Lower security settings for the *Autoprint* user and change registry settings for Autoprint with a file from the Picis web site. Contact Picis Support for further information.

See “Administrator information about the Outlook e-mail security update” at http://support.microsoft.com/kb/263296 for more information on Outlook security updates.

10

Database Backups

Backup Strategy

The first rule is to assume that system failure is inevitable—it is not a case of *if* the hardware fails, but *when* the hardware fails. You should perform regular backups to keep your system running smoothly and protect it against system failure. This chapter offers recommendations on setting up backups and when they should run.

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

- SQL Server hardware
- SQL databases
- Servers/transaction processors
- Spare hardware

SQL Server Hardware

Many sites setup SQL Server redundancy through mirror imaging. This means that all data written to the active servers is simultaneously written to identical backup servers. Should processing fail on one server, its mirror automatically takes over, thus reducing or eliminating downtime.

In order to avoid the expense of mirroring, you may opt to have a single spare SQL server. When the hardware fails you restore database backups to the spare server and resume operations. This strategy involves some downtime as you restore backups to the spare server, and data entered since the last backup must be re-entered on the spare server.

SQL Server Database Backups

There are three types of backup jobs that can be configured to help protect data. The backup job(s) can be set up at any time using the SQL Server Maintenance Plan Wizard or using a standard backups scripts/processes 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 six days of the week when the full backup does not run, at the same time specified for full backups, if daily. If differential backups are run hourly, they should run every hour excluding the hour at which the full backup runs.
- **Transaction**- performed hourly, or every X number of minutes, if differential backups run 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: Sites are responsible for setting up their own backup jobs. It is critical that a backup plan be configured and monitored by the site. Picis will not be liable for any errors or data loss resulting from not implementing appropriate backup, restore, and maintenance procedures and policies.

Setup Backup Jobs

Backup jobs are not automatically setup by Picis during installation—they must be setup by the site. This is coordinated with sites ahead of time.

To setup a backup job (or jobs), sites may use the SQL Server Maintenance Plan Wizard or may implement the same backup scripts/processes used for other database servers in their organization.

When planning to setup the backup jobs, you should select a time of day when the backup is least likely to interfere with normal processing.

Note: To receive emails when jobs fail and/or succeed, a SQL Server Database Mail profile must be setup prior to installing or upgrading to version 8.6.x; Database Mail setup is the responsibility of the site.

Note: In order to reduce space consumed by backups, consider using compression. This option can be set at the server level so all backups are compressed 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, first back up the end of the log file (the transactions that were written since the last log file backup was performed). In SQL Server, this can be accomplished by choosing **Backup Type** > **Transaction Log**, and then on the Options 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 a day has passed 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 fires (by default, hourly). This frequency can be changed when the job is set up. Keep in mind that decreasing the frequency will cause larger gaps of possible data loss if you need to restore.
5. If you were able to back up the tail of the log (see step 1), then restore that backup; otherwise (if possible) repeat the transactions 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.

Servers/Transaction Processors

Although no critical data is stored on 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.

11
Maintenance Jobs

Maintenance Jobs Overview

This chapters gives guidelines for routine maintenance of your Perioperative and Critical Care system. Maintenance topics include:

- *SQL Server Maintenance* below
- *Stop and Restart SQL Server Services* on the next page
- *Stop (or Restart) Background Servers* on page 121
- *Provided SQL Server Agent Jobs* on page 123
- *Customer Required SQL Server Agent Jobs* on page 126
- *Downloading Files From the Picis FTP Site* on page 126
- *Maintenance Schedule* on page 127

SQL Server Maintenance

Daily maintenance of your SQL Server consists of two tasks:

- Viewing the server error log for the SQL Server. (See the help file for your SQL Server version for instructions on accessing this log).
- Viewing the event viewer application log for the machine on which the SQL Server resides. (See the operating system help file for instructions on accessing this log).

Interpret the SQL Server Error Log

Browse through the SQL Server Error Log looking for errors. (Backup and Transactions listed in the Error Log are normal).

Interpret the Application Log

In the first column of the log, you see entries with blue, yellow, or red circles.

- Blue is Informational. There was nothing wrong with this event.
- Yellow is a Warning. Double-click the event to see details about the warning.
- Red indicates a Critical problem. Double-click on the event to see details about the problem. Red circles often identify a licensing issue that should be resolved by your IT staff.

Any events in Red or Yellow 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 server, SQL Servers need to be stopped just before doing so and then restarted.

Stopping SQL Server services before rebooting the server

Stop the SQLAgent 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, reboot the server.

Restarting SQL Server services after rebooting the server

After the server has rebooted, restart SQL Services and refresh the database list following the instructions in the Microsoft SQL Server Management Studio help file.

If any databases are shown disabled after the database list has been refreshed (in gray instead of gold), please log a Service Request; do not restart extracts, syncs, or autoprints and do not let users use the system.

Stop (or Restart) Background Servers

As part of routine maintenance or while troubleshooting it may be necessary to stop or restart one or more background servers. The integrated nature of Perioperative and Critical Care software means that stopping one server may mean other servers need to be stopped to maintain system integrity. Use the following notes as guidelines when stopping or restarting your servers.

- **Frequency**: Picis recommends following Microsoft's advice of rebooting servers on a monthly basis
- **Stopping the Database Server**: Prior to stopping the Database Server all other servers should be stopped. Users also need to log out.
- **Stopping a Transaction Processor**: Prior to stopping a Transaction Processor all executable should be stopped.
- **Stopping the PMR Server**: Prior to stopping the PMR server the external systems should stop sending messages.
- **Stopping Picis Network Server**: Prior to stopping the Network Server the external systems should stop sending messages. Users can continue working, but may experience slower performance and will not be able to print from Anesthesia Manager, PACU Manager, or Critical Care Manager.

Important Notes

- From the moment extracts or syncs are stopped, interface data is no longer available in Picis Perioperative and Critical Care applications until they are restarted, after which it takes time to catch up. The less downtime, the better.
- If only the application server needs to be rebooted, then only the jobs on that application server need to be stopped.
- If the SQL Server is to be rebooted, then you need to follow all of the steps in this topic.

Stopping background servers

This procedure uses the Live environment from the *Standard Server Configuration* on page 11 as a reference.

1. Ensure all users are logged off all Perioperative and Critical Care applications.
2. Stop all inbound communications from the external systems (ADT, Material Management and Laboratory systems etc.).
3. Stop the server hosting PMR.
4. Stop the Picis Network Server.
5. Stop Surgsync and note any error messages:
   - From the task bar double-click the CareTaker icon (blue bubble).

  - Clear the box next to **Surgsync.exe**.
6. Stop the server hosting Surgsync.
7. Stop Autoprint and note any error messages:
   - From the task bar double-click the CareTaker icon (blue bubble).
   - Clear the box next to **Autoprint.exe**.
8. Stop the server hosting Autoprint.
9. Stop the Database Server:
   - On the Windows Task Bar, double-click the SQL Server icon.
   - Next to **Server**, select the Database Server. (It should be selected by default).
   - Next to **Services**, select the SQL Server. (It should be selected by default).
   - Click the **Stop** button ■.
   - Click the **X** in the top right hand corner to close the SQL Server Service Manager.

Starting system servers

This procedure uses the LIVE environment from the *Standard Server Configuration* on page 11 as a reference.

1. Start the Database Server:
   The database server may automatically start; if it does not, follow this procedure:
   - On the Windows Task Bar, double- click the SQL Server icon.
   - Next to **Server**, select the Database Server. (It should be selected by default).
   - Next to **Services**, select the SQL Server. (It should be selected by default).
   - Click the **Start** button ▶.
   - Click the **X** in the top right hand corner to close the SQL Server Service Manager.
2. Start the server hosting Autoprint:
   Depending on the CareTaker configuration the Autoprint server may automatically start; if it does not, follow this procedure:
   - On the task bar, double-click the CareTaker icon (blue bubble) to start CareTaker.
   - Select the box next to **Autoprint.exe**.
3. Start the server hosting Surgsync:
   Depending on the CareTaker configuration the Surgsync may automatically start; if it does not, follow this procedure:
   - On the task bar, double-click the CareTaker icon (blue bubble) or start CareTaker.
   - Select the box next to **Surgsync.exe**.
4. Start the Picis Network Server:
   Depending on the Server Service configuration PCM and the Printouts Service may automatically start; if they do not, follow this procedure:

- In the Administrative Tools folder for Windows, click **Services**.
  (This folder will either be in the Control Panel or in the Programs folder of the Start menu).
- Right-click the service name and select **Start**.
- Click **OK**.

5. Start the server hosting PMR.

Provided SQL Server Agent Jobs

The following jobs are created and set up as standard by DB Utility.

If a job fails, notify Picis support.

PSM database

Database/Job	Description	Frequency
<db name>__Transaction_Mon	Searches and kills open transactions with no activity for more than a pre-determined number of hours. (Default set to 12 hours.)	Hourly
<db name>__PIMS_Hourly_Purge	Purges any expired record from the PIMS tables	Hourly

ORM database

Database/Job	Description	Frequency
<db name>__Transaction_Mon	Searches and kills open transactions with no activity for more than a pre-determined number of hours. (Default set to 12 hours.)	Hourly
<db name>_truncate_temp_ext_report'	Truncates temporary external report table to avoid Crystal Reports error. Also updates nextnumber table for temp_ext_report.	Daily (midnight)
<db name>_booking_auto_email_reminder	Pulls list of bookings that need reminder emails X days in advance, from booking_auto_email_audit_trail and sends each to email stored proc.	Daily (4:00 AM)

Database/Job	Description	Frequency
<db name>_purge ORM pre-reg tables	Purges processed ADT outbound booking data from the *booking_affi_ adt_data* and *booking_ affi_ adt__data_multi* tables.	Weekly (Sunday 1:00 AM)

IDB database

Database/Job	Description	Frequency
<db name>__Transaction_Mon	Searches and kills open transactions with no activity for more than a pre-determined number of hours. (Default set to 12 hours.)	Hourly
IDB Daily Purge <Interface name>(<db name>) *e.g. IDB Daily Purge NUR (interface)*	Calls stored procedures to purge data if the corresponding data has been purged from the HIS.	Daily
IDB Weekly SQL Storage Analysis <db name>	Created from idb_jobs_add SQL Storage Analysis	Weekly

TRK database

Database/Job	Description	Frequency
<db name>__ Transaction_Mon	Searches and kills open transactions with no activity for more than a pre-determined number of hours. (Default set to 12 hours.)	Hourly
<db name>_LU_Process_ TxQ	Processes activity off of a work queue and updates the tracking screens. Though the schedule is set to every minute, the job actually runs continuously to process entries off of the work queue. The work queue consists of activity within SmarTrack. There is a two second delay between iterations of processing of the work queue data.	Continuous

Database/Job	Description	Frequency
<db name>_Regular_ Maintenance	Performs routine maintenance on SmarTrack queues, e.g. cleans up beeper queues, redraws schedules, etc. Though the schedule is set to every minute, the job actually runs continuously to process entries off of the work queues. There is a two second delay between iterations of processing of the queue data.	Oncer per minute
<db name>_BKG_ Process_TxQ	Initiates the processing of work queues used to update patient demographic data with any changes. It also initiates the processing of the telephony work queue, if applicable. Though the schedule is set to every minute, the job actually runs continuously to process entries off of the work queues. There is a two second delay between iterations of processing of the work queue data	Continuous

Continuous TRK db Jobs

The job status reflects the result of the last execution of the job. For continuous jobs, the status may appear as *Failed* if the job was previously shut down improperly. If the job repeatedly fails (seen in the job history), contact Picis Support.

Example: The SQL Server machine is rebooted before stopping SQL Server Agent. Manually stopping and starting the job will reset the status.

Missing or Additional Jobs

If any the jobs listed above are not installed on your database server, or you have additional jobs, contact your Picis Implementation representative for clarification as to the purpose of these jobs.

Confirming a database job has successfully executed

1. At the database server, click **Start** > **Programs** > **Microsoft SQL Server** > **SQL Server Management Studio**.
2. Click the plus sign next to your database server.
3. Click the plus sign next to the **Management** folder and then click **Jobs**.

   The status of the job is displayed in the Status column.

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 equivalent jobs for the TEST environment.

Below is a summary of the required maintenance jobs.

Database/Job	Description	Recommended Frequency
Defragmentation	Analyzes the table fragmentation in each database and defragments the databases accordingly. For more information on table fragmentation, see Microsoft help.	Weekly
Integrity check	Checks for database inconsistencies. For more information on table fragmentation, see Microsoft help.	Weekly
Update statistics	Updates 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 help.	Weekly

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

Downloading Files From the Picis FTP Site

Pre-requisite: In order to use the Picis FTP site, you must first obtain a user name and password from your Picis representative.

Downloading files from the Picis FTP site

1. In a web browser, navigate to *ftp-us.picis.com*.

   If it is the first time you have accessed the site, you will be prompted for a user id and password.
2. Enter your **User Name** and **Password**, then click **Login**.

   A window showing the folders on the FTP site appears.
3. Double-click the “Public” folder.

   The folders within the “Public” folder appear.
4. Double-click the “Download” folder.

   The files and folders within the “Download” folder appear.

   If you see the file you need, go on to the next step. If not, you may have to open some of the folders in the window to find the file.
5. Double click the file you want.

   The File Download Screen appears.
6. Select **Save File To Disk**, then click **OK**.

   The Save As dialog box appears.
7. Click the down arrow at the **Save in** prompt, select **Network Neighborhood**, then select your SQL server.
8. Double-click your SQL server, then double-click your “Public” folder, and then click **Save**.

   A progress bar appears as the file downloads.
9. Make sure the files download completely by noting the file size on the FTP web site and then comparing it to the size of the file you downloaded into your “Public” folder.
10. Send an email confirmation to your Picis representative when all files are downloaded.

Maintenance Schedule

The following table gives you an example maintenance schedule for your Picis Perioperative and Critical Care system. Tasks are organized based on when they should occur:

- *Several Times per Shift* on the next page
- *Hourly* on the next page
- *Once a Day* on the next page
- *Once a Week* on page 129
- *Once a Month* on page 129

Note: This is only an example. You may need to tailor this schedule to your own requirements. See *Maintenance Jobs* on page 119 for detailed information on system maintenance.

Several Times per Shift

Task	Details
Check HL7 ADT Interface	Ensure transactions are processing and that transactions are marked with 'successful.' Make sure that there are few or no unprocessed transactions (many unprocessed transactions in a queue would indicate a bottleneck).
Check Extracts	For Meditech HIS only: ensure that all extract Windows are open and that data is processing. Check last update date and time to ensure that data is current.
Check Surgsync	Check at least one full cycle of synchronization. Make sure there are no errors seen on the screen.
Check Autoprint	Observe Autoprint to see jobs processing. Note messages while processing such as 'cannot find device'. View Autoprint queue to ensure no jobs in queue (many unprocessed transactions in a queue would indicate a bottleneck).

Hourly

Task	Details
Check the Database jobs	Ensure that defined hourly database jobs have successfully completed. See *Confirming a database job has successfully executed* on page 125 for details of how to check a database job. See *Customer Required SQL Server Agent Jobs* on page 126 for a list of hourly database jobs.

Once a Day

Task	Details
Check the Database jobs	Ensure that defined daily database jobs have successfully completed. See *Confirming a database job has successfully executed* on page 125 for details of how to check a database job. See *Customer Required SQL Server Agent Jobs* on page 126 for a list of hourly database jobs.

Task	Details
Check HL7 ADT Error Logs	Check HL7 Messenger Error Logs. A number of error messages are normal as the ADT interface routinely rejects certain messages. Determine the normal size of the reject/error log file for your site and ensure there is no log file that is substantially larger than the normal error log file.
Ensure third-party backups ran successfully	Ensure the scheduled backup of the SQL backup files to other media (e.g. tape) ran successfully.
Ensure all scheduled Virus Scans ran successfully.	Ensure virus scans run on the SQL Server(s) and all transaction processors. See details in this manual regarding files to exclude when running the virus scans on the SQL server.

Once a Week

Task	Details
Check the Database jobs	Ensure that defined weekly database jobs have successfully completed. See *Confirming a database job has successfully executed* on page 125 for details of how to check a database job. See *Customer Required SQL Server Agent Jobs* on page 126 for a list of hourly database jobs.
Check SQL Database free space	Ensure that all databases have free space remaining. Databases should be set to 'autogrow' and free space is managed by the SQL Database. Ensure the databases are growing appropriately as necessary.
Check SQL Database Growth and Free Disk Space on SQL server	Establish a baseline for future growth and ensure enough free disk space is available for comprehensive database growth. Any substantial decreases in disk free space should be noted and investigated further.
Back up or image Transaction Processors	Although no critical data is stored on the transaction processors, it is recommended that you periodically backup or image the active transaction processors to speed recovery should a device fail.

Once a Month

Task	Details

Task	Details
Check Disk Free Space on Transaction Processors	Ensure at least 1 GB of free space exists on the appropriate drive partition(s) where the applications are functioning on each of the transaction processors. Any substantial decrease of free disk space should be investigated to determine the cause.
Reboot SQL Server(s) and CareSuite background servers	See *Stop (or Restart) Background Servers* on page 121 for full more details.
Delete old HL7 log files	Log files for the HL7 ADT messenger are stored in folders by log date. Delete old log files to free up space on the transaction processor. **Note:** If you have heavy ADT messaging volume (more than 2000 message per day) you may want to purge ADT log files more often.

12

SQL Server Password Configuration

The Perioperative and Critical Care applications use a single SQL login when connecting to the databases on the SQL Server machine(s). The login is delivered with sufficient rights, allowing the applications to connect, read, and update data in all of the system databases.

System administrators, or users with the required rights, have the ability to change the SQL login password through the SQL Login UI. Users can access the SQL Login UI through a URL that is hosted on the server where the Picis (web) 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 this password affects all system databases in all instances on the SQL server; Perioperative and Critical Care applications do not need to be manually updated with the new password.

Note: The SQL login that is setup with version 8.6.x 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.

- Have system administrator rights on the SQL Server(s) that will be affected by the password change (for example, if both a Database server and Extelligence server exist, the user must have the appropriate rights to both SQL servers).

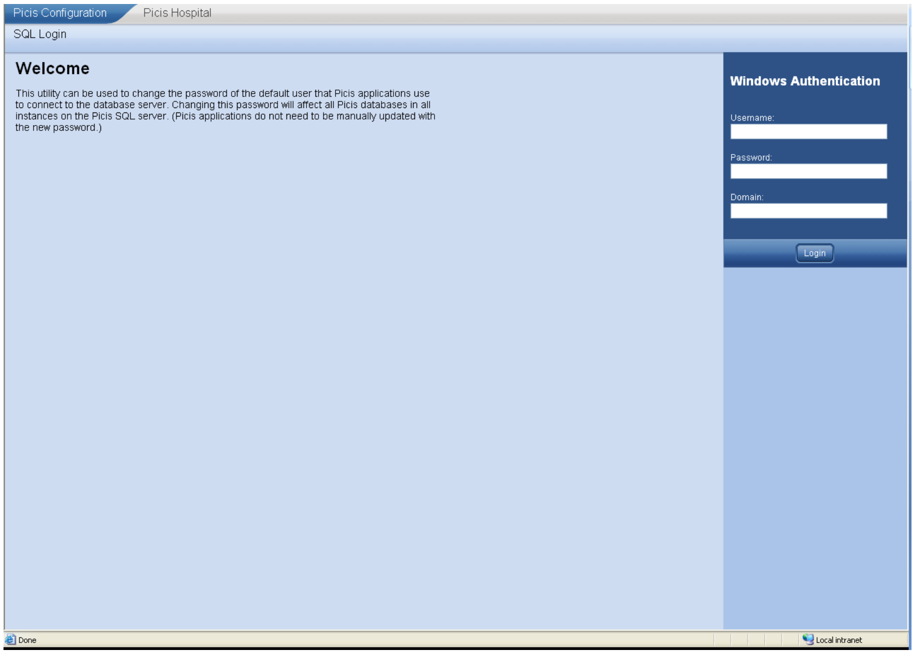
Note: New passwords must be at least eight characters long and contain both a letter and a number.

Changing the SQL login password

1. Go to: http://<PicisServicesServer>/LoginSQLUI/Default.aspx.

   where <PicisServicesServer> is the name of the Picis (web) Services server.

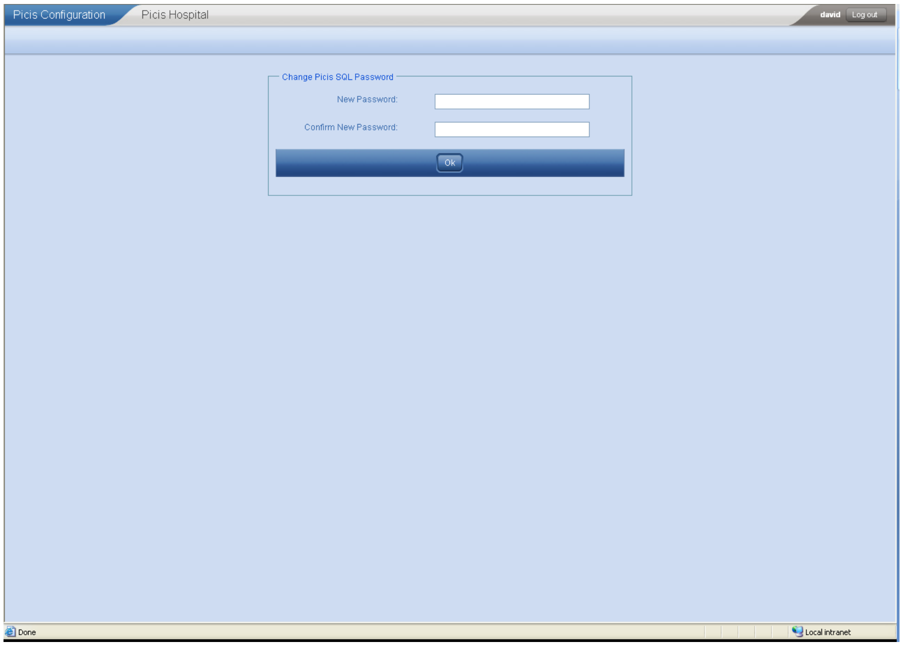
   The Welcome page appears.



This utility can be used to change the password of the default user that Picis applications use to connect to the database server. Changing this password will affect all Picis databases in all instances on the Picis SQL server. (Picis applications do not need to be manually updated with the new password.)

2. Type the **Username**, **Password**, and **Domain**, of the user with rights to change the password in the corresponding fields, and click **Login**.

   The Change SQL Password page appears.



3. Type the new password and then re-type the password to confirm, then click **OK**.

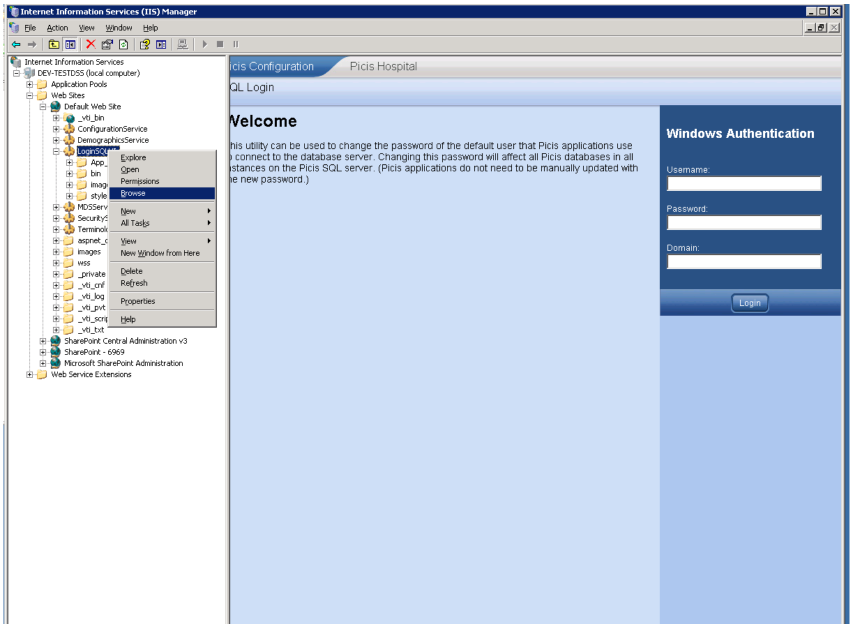
   A confirmation message should appear that the password has been changed successfully.

4. Close the window.

Troubleshooting

As this is a website, IIS must be running to access the SQL Login Password Configuration page. Check the Internet Information Services Manager to ensure the folder “LoginSQLUI” exists.

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



Velcome

his utility can be used to change the password of the default user that Picis applications use connect to the database server. Changing this password will affect all Picis databases in all stances on the Picis SQL server. (Picis applications do not need to be manually updated with e new password.)

Username:

Password:

Domain:

13

Reportuser SQL Trace

SQL Trace Overview

A single SQL user has been created for use with Picis Perioperative and Critical Care 8.6.x; any additional SQL users that existed for Perioperative and Critical Care products prior to this release are no longer supported and will eventually be removed (with the exception of reportuser). The reportuser will remain in place and will continue to be usable if the user existed at your site in a previous version, but it is no longer delivered or supported.

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

In the steps below, "reportuser" is the SQL user being traced. To capture the activity of the reportuser, a server-side trace should be run on the SQL Server to create a trace file of the required activities listed below:

- Reportuser login/logout
- Objects used by reportuser
- Queries run by reportuser

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

Trace SQL User Activity

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

Tracing user activity

1. Choose a trace method.

Method A	Edit the required parameters in the sample script that has been provided and then run the script to perform the trace. To use this method, browse to "\Non DB Utility Files\Useful SQL*Sample user activity trace procedure.sql*" (available in the release package). To edit the sample procedure, search/replace the code for the following parameters:
Method B	Manually create a trace based on the required components. To manually create the trace, use the commands noted in section *Required Trace Components* on the facing page.

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 trace manually* below.
Method B	Configure the trace to start automatically when the SQL Server is restarted. For the required script information, see section *Configuring the trace to start automatically with SQL Server restart* on the facing page.

Starting and stopping a trace manually

- To manually start the trace, run the following script against the SQL Server (where "dbo.sp_reportuser_trace" is the procedure name):

```
exec <dbo.sp_reportuser_trace>
 GO
```

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

- To stop the trace, run the following script against the SQL Server (where "traceid" is the value of the trace):

```
sp_trace_setstatus [traceid], 0
```

Configuring the trace to start automatically with SQL Server restart

- Run the following command from the SQL Server Management Studio to configure an auto-trace to run every time the SQL Server is restarted (where “dbo.sp_reportuser_trace” is the procedure name).

```
declare @rc int
exec @rc = sp_procoption '<dbo.sp_reportuser_trace>', 'startup', 'on'
IF @rc != 0
BEGIN
 print 'ERROR: sp_procoption returned ' + CAST(@rc AS NVARCHAR(10))
 print 'ERROR: Could not set <sp_reportuser_trace> for autostart'
END
```

Note: If you copy the code above directly from this document, be sure to check the resulting text and confirm it appears exactly as it does in this document.

Required Trace Components

If you choose to create a trace manually based on the required components, use the following parameters to specify the trace.

Parameters to create the trace	
`Trace ID`	The ID of the trace
`Options`	Various options that can be set
`TraceFile`	Physical file name where you want to write the trace file
`MaxFileSize`	Size of the file, before closing and creating subsequent files
`StopTime`	Time to stop the trace

Note: For reference, see the Microsoft article "ms190362" or click here for a direct link: http://msdn.microsoft.com/en-us/library/ms190362(SQL.90).aspx.

Parameters to specify the events to capture	
`Trace ID`	The ID of the trace
`EventID`	The ID of the event you want to capture

Parameters to specify the events to capture	
`ColumnID`	The ID of the column you want to capture
`On`	Whether you want to turn this event on or off

Note: For reference, see the Microsoft article "ms186265" or click here for a direct link: http://msdn.microsoft.com/en-us/library/ms186265(v=SQL.90).aspx.

Parameters to filter the data that is retrieved	
`Trace ID`	The ID of the trace
`ColumnID`	The ID of the column you want to set the filter on
`Logical Operator`	Specifies whether this is an AND or OR operation
`ComparisonOperator`	Specifies whether the value is equal, greater than, less than, like, etc.
Value	The value to use for your comparison

Note: For reference, see the Microsoft article "ms174404" or click here for a direct link: http://msdn.microsoft.com/en-us/library/ms174404.aspx.

Parameters to specify the start/stop of the trace	
Trace ID	The ID of the trace
Status	Stop, start, or close a trace

Note: For reference, see the Microsoft article "ms176034" or click here for a direct link: http://msdn.microsoft.com/en-us/library/ms176034(v=SQL.90).aspx.

14

Picis Configuration Wizard

Picis Configuration Wizard Overview

The Picis Configuration Wizard is used to review or change the configurations of a machine that has “clinical modules” components installed. By default, the required components are installed in the following locations, respectively:

Windows 7- “C:\Program Files (x86)\Picis\Bin”
Windows Server- “C:\Picis\Diagnostics”

Note: Administrative rights are required to run the Picis Configuration Wizard.

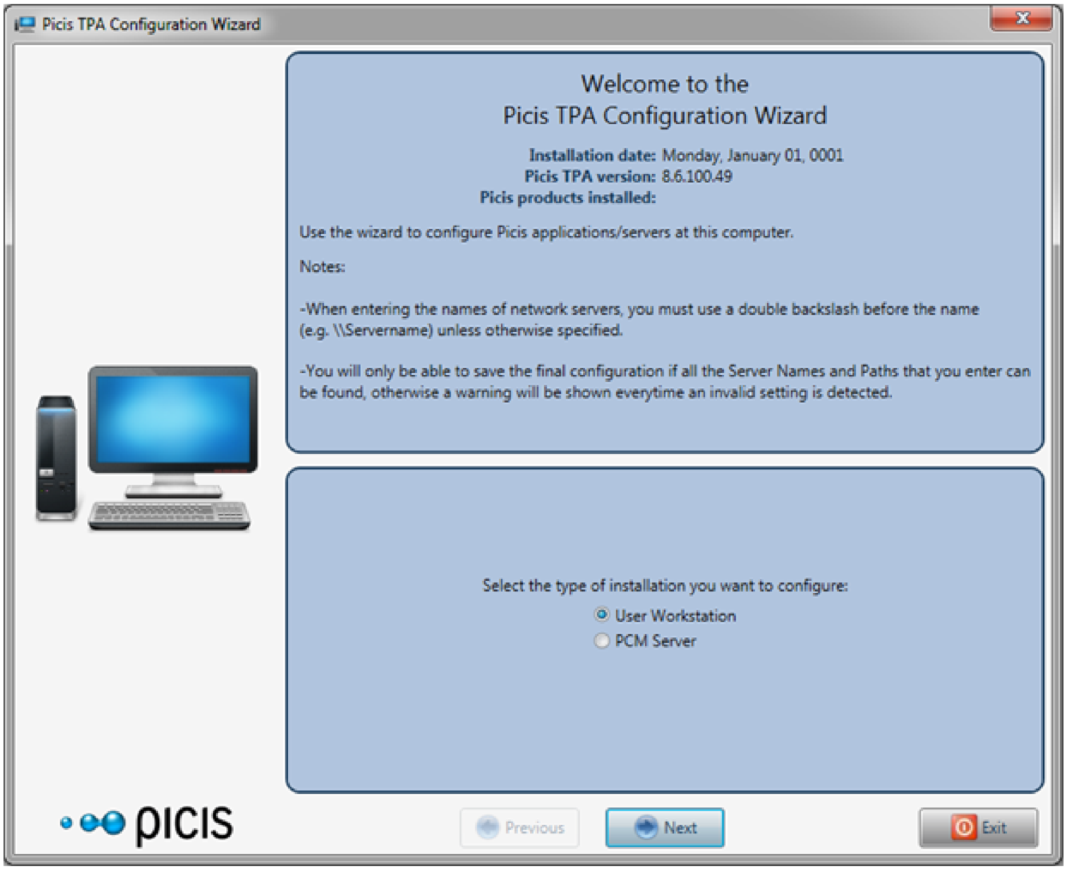
Note: The Picis Configuration Wizard must be accessed from the machine that requires configuration.

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

- *Configuring a User Workstation* on the next page.
- *Configuring the PCM Server* on page 141.

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

- ConfigToolUI- the wizard where users input data.
- ConfigTool command line- carries out the actions based on the parameters entered in the UI.



Welcome to the
Picis TPA Configuration Wizard

Installation date: Monday, January 01, 0001
Picis TPA version: 8.6.100.49
Picis products installed:

Use the wizard to configure Picis applications/servers at this computer.

Notes:

-When entering the names of network servers, you must use a double backslash before the name (e.g. \\Servername) unless otherwise specified.

-You will only be able to save the final configuration if all the Server Names and Paths that you enter can be found, otherwise a warning will be shown everytime an invalid setting is detected.

Select the type of installation you want to configure:

● User Workstation
○ PCM Server

There are two text files that are generated by the ConfigTool components, which are helpful when troubleshooting:

- *ConfigToolUI.log*- UI log file to be used with any issues before you click the Finish button in the ConfigToolUI.
- *ConfigTool.log*- the file generated by the ConfigTool command line utility, which is started after the users click the Finish button in the ConfigToolUI. Reference this file for issues when applying the configuration changes.

Configuring a User Workstation

1. Browse to the “C:\Program Files (x86)\Picis\Bin" folder and double-click *ConfigToolUI.exe* to launch the Picis Configuration Wizard.
2. Select **User Workstation** and click **Next**.

   The Picis (web) Services window appears.
3. Enter the name of the Picis (web) Services server and click **Next**.

> **Note:** If the name of the Picis (web) Services server is changed, the ConfigToolUI must be restarted; in this case, click **Yes** to restart the tool. The Picis (web) Services window appears with the new server name. Click **Next** to continue.

The Department, Facility, and Location window appears.

4. Specify the Department, Location, Initials, and Workstation Type.

   (optional) To add a new department, select "I want to add a new department" and enter the required details in the available fields.
5. Click **Next**.

   The Summary window appears. Review the Configuration Summary to make sure the settings are accurate.
6. Click **Finish**.

   A confirmation window appears.
7. Click **Yes** to proceed and, upon notice of a successful configuration, click **OK** to exit.

   OR

   Click **No** to return to the Summary window and edit the settings.

Configuring the PCM Server

1. At the PCM server, stop the PCM.NET and Central Print Service services.
2. Browse to the "C:\Picis\Diagnostics" folder and double-click *ConfigToolUI.exe* to launch the Picis Configuration Wizard.
3. Select **PCM Server** and click **Next**.

   The Picis (web) Services window appears.
4. Enter the name of the Picis (web) Services server 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 and, upon notice of a successful configuration, click **OK** to exit.

   OR

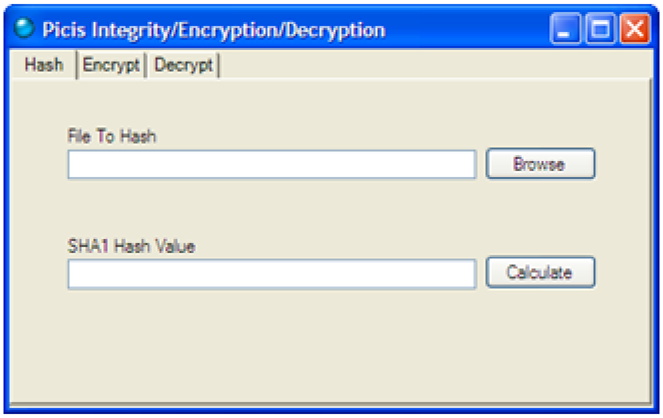
   Click **No** to return to the Summary window and edit the settings.
7. Restart the PCM.NET and Central Print Service services.

15

Crypto Tool

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 Perioperative and Critical Care applications to ensure their confidentiality and protect their contents. This tool is mainly intended for use with files that will be sent to an external system, but can also be used to protect local or network-share files.



- **Hash** generates a unique value for a file to ensure that its integrity has not been compromised. After a hash value is generated, you should save a copy in a reliable location for reference.
- **Encrypt** encodes a file to protect its contents.
- **Decrypt** decodes a file so only users with the required password can access its contents.

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

Access the Crypto Tool

The Crypto Tool (*PicisCrypto.exe)* is available upon request.

Hash, Encryp, or Decrypt a File

Hashing, encrypting, or decrypting a file requires access to the Crypto Tool. See *Access the Crypto Tool* above for details on accessing the tool.

Generating a Hash Value

1. Open the Crypto Tool either by double-clicking the file *PicisCrypto.exe* or from a menu within the application.

   The Crypto Tool 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 word-processing application) to retain the value.

   Refer to the saved hash value when checking the file's integrity at a later time.

Encrypting a File

1. Open the Crypto Tool either by double-clicking the file *PicisCrypto.exe* or from a menu within the application.

   The Crypto Tool 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 Encrypt using AES field. By default, the encrypted file is saved to the same location where the original file exists (with the suffix “.encrypt”). To change the encrypted file's destination, click the **Change** button and specify a new path.

5. Type a password for the encrypted file, and then re-type the password to confirm its accuracy.

> **Note:** This password is required to decrypt the file.

6. Click **Encrypt**.

   A message appears, confirming the successful encryption.

Decrypting a File

1. Open the Crypto Tool either by double-clicking the file *PicisCrypto.exe* or from a menu within the application.

   The Crypto Tool appears.
2. Click the **Decrypt** tab.
3. Click the **Browse** button and find the file you want to decrypt.
4. Select the file and click **Open**.

   The path appears in the File To Decrypt using AES field. By default, the decrypted file is saved to the same location where the original file exists. To change the decrypted file's destination, click the **Change** button and specify a new path.
5. Type the password that was created when the file was encrypted, and then re-type the password to confirm its accuracy.
6. Click **Decrypt**.

   A message appears, confirming the successful decryption.

15

Crypto Tool

Hash, Encryp, or Decrypt a File

16

Meditech Extracts

Meditech Extracts Overview

For sites integrated with a Meditech HIS system, Meditech extracts pull data from that system into the Interface database (a one-way process).

Meditech Modules

Data may be pulled from the following Meditech modules:

- MIS
- Admissions
- Medical Records
- Billing/Accounts Receivable
- Materials Management
- Scheduling
- Lab
- Nursing

Each Meditech module requires its own set of extracts.

Magic and VMagic Extracts

Extracts operate on both Magic and Meditech's proprietary VMagic client-server platforms.

Extracts on Magic platforms have two parts:

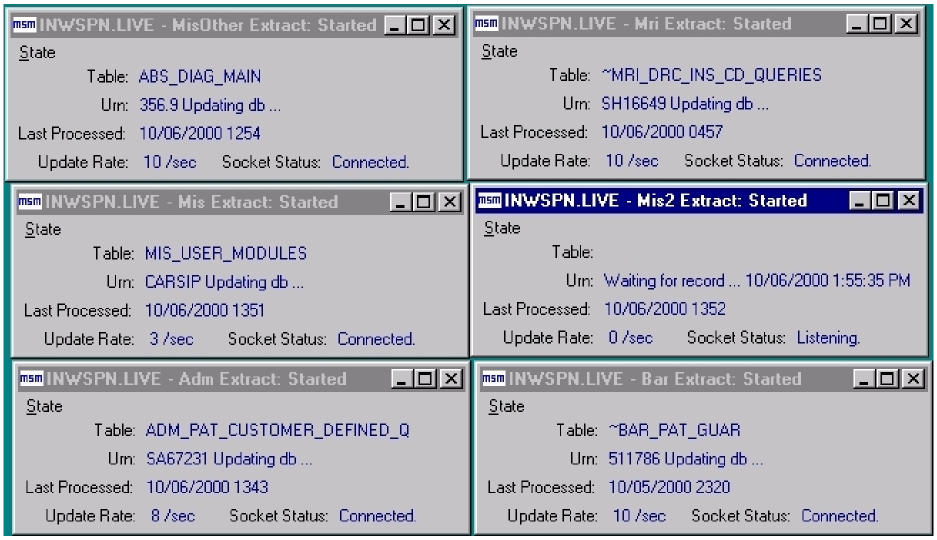
1. A Magic job on the Meditech mainframe reads the data.
2. A Picis extract program on the transaction processors reads data from the Magic job and stores it in the Interface database.

On VMagic platforms, Picis extracts on transaction processors, then both read the data from Meditech and store it in the Interface database.

Extract Status Message Boxes

The extract programs receive Meditech data and file it into the SQL database. An Extract Status Message Box is displayed for each extract. It is best to leave the Status Boxes displayed on the desktop so you can easily check the extracts.

This is an illustration of VMagic extracts running on a transaction processor. Magic extracts are similar.



```
INWSPN.LIVE - MisOther Extract: Started
State
            Table:  ABS_DIAG_MAIN
              Urn:  356.9 Updating db ...
   Last Processed:  10/06/2000 1254
      Update Rate:  10 /sec     Socket Status:  Connected.

INWSPN.LIVE - Mri Extract: Started
State
            Table:  ~MRI_DRC_INS_CD_QUERIES
              Urn:  SH16649 Updating db ...
   Last Processed:  10/06/2000 0457
      Update Rate:  10 /sec     Socket Status:  Connected.

INWSPN.LIVE - Mis Extract: Started
State
            Table:  MIS_USER_MODULES
              Urn:  CARSIP Updating db ...
   Last Processed:  10/06/2000 1351
      Update Rate:  3 /sec      Socket Status:  Connected.

INWSPN.LIVE - Mis2 Extract: Started
State
            Table:
              Urn:  Waiting for record ... 10/06/2000 1:55:35 PM
   Last Processed:  10/06/2000 1352
      Update Rate:  0 /sec      Socket Status:  Listening.

INWSPN.LIVE - Adm Extract: Started
State
            Table:  ADM_PAT_CUSTOMER_DEFINED_Q
              Urn:  SA67231 Updating db ...
   Last Processed:  10/06/2000 1343
      Update Rate:  8 /sec      Socket Status:  Connected.

INWSPN.LIVE - Bar Extract: Started
State
            Table:  ~BAR_PAT_GUAR
              Urn:  511786 Updating db ...
   Last Processed:  10/05/2000 2320
      Update Rate:  10 /sec     Socket Status:  Connected.
```

1. The top line on each extract shows the extract database and name.
2. The second and third lines show the SQL table and data value currently being written.

> **Note:** The **URN** line also shows errors. If the “Filing Error” error message appears constantly, contact Picis support.

3. The **Last Processed** line shows the time of the last update on the Meditech side. This time should be within 10 - 15 minutes of the current time.
4. **Update Rate** is the number of records per second being processed.
5. **Socket Status** can have one of two messages:

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

Turning off Interfaces (Magic Side)

1. From the IDB Menu (it may also be called the CS Interface Magic Extract Menu) choose **Support Process IDB Interface Extract Jobs**
2. Use the arrow keys to navigate. Toggle jobs off using the space bar.

   It may take a few minutes for all the jobs to shut down but they will eventually stop. You may need to press <R> to refresh the display.

Turning off Interfaces (Workstation Side)

1. Right-click CareTaker (lower right) then choose **Show CareTaker**.
2. Click each job to deselect it or choose **Deselect All** to shut off all jobs.

   The windows will shut down one at a time. To reverse this process, click each job to check or choose **Select All** then choose **Hide Form**.

17

TallMan Medication Update Overview

The TallMan Medication update will change medication description case to match the case approved by the FDA and ISMP. An example of an update would be changing the description from *OXYCONTIN* to *OxyCONTIN*. For sites that choose to use TallMan Letters the CAR and ORM databases are updated using scripts provided by Picis.

CAR Database

The script to update the CAR database will update the Medications and the Treatments database table. In the Medications table the Medicationdesc column is updated to match TallMan case. In the Treatments table the Genericname column is updated to match TallMan case.

Note: The script may generate a message indicating that it cannot be run because of duplicate descriptions (these are case-sensitive) have been found in the Medications database table. If duplicates are found they will need to be resolved before the script is re-run.

ORM Database

The script to update the ORM database will update the Allergy database table. In the Allergy table the All_desc column is updated to match TallMan case.

Running the TallMan Medication Update

1. Browse to the folder: "\Non DBUtility Files\GroupSpecificScripts\CAR."
2. Run the CAR TallMan medication update script, *Update Medication Descriptions to TallMan Case.sql*.

3. Browse to the folder: “\Non DBUtility Files\GroupSpecificScripts\ORM.”
4. Run the ORM TallMan medication update script, *Update Medication Descriptions to TallMan Case.sql*.

18

Technical Notes

Technical Notes Overview

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

File Save Restriction

Some Perioperative and Critical Care programs include functionality for saving files. Users may find that it is not possible to save the files to certain local folders, such as the "Program Files" folder. This is due to the Windows 7 operating system feature called User Account Control (UAC), which is enabled by default. Sites can disable UAC at workstations, subject to their own security policy. If a site chooses not to disable UAC it should make users aware of the restrictions. For more information on UAC, see:

http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx

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

External Report Scheduler

In External Report Scheduler one of the export options is to a shared network location. The Picis Report Service (PRS) generates the reports and runs on the administrative server where Picis (web) Services are installed. There must be connectivity between the shared network location and the administrative server in order for the report to be exported.