



**Epicor ERP**  
**System Administration Guide**  
**10.2.700**

## **Disclaimer**

This document is for informational purposes only and is subject to change without notice. This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication. However, Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims any applicable implied warranties, such as fitness for a particular purpose, merchantability, satisfactory quality or reasonable skill and care. As each user of Epicor software is likely to be unique in their requirements in the use of such software and their business processes, users of this document are always advised to discuss the content of this document with their Epicor account manager. All information contained herein is subject to change without notice and changes to this document since printing and other important information about the software product are made or published in release notes, and you are urged to obtain the current release notes for the software product. We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice. The usage of any Epicor software shall be pursuant to an Epicor end user license agreement and the performance of any consulting services by Epicor personnel shall be pursuant to Epicor's standard services terms and conditions. Usage of the solution(s) described in this document with other Epicor software or third party products may require the purchase of licenses for such other products. Where any software is expressed to be compliant with local laws or requirements in this document, such compliance is not a warranty and is based solely on Epicor's current understanding of such laws and requirements. All laws and requirements are subject to varying interpretations as well as to change and accordingly Epicor cannot guarantee that the software will be compliant and up to date with such changes. All statements of platform and product compatibility in this document shall be considered individually in relation to the products referred to in the relevant statement, i.e., where any Epicor software is stated to be compatible with one product and also stated to be compatible with another product, it should not be interpreted that such Epicor software is compatible with both of the products running at the same time on the same platform or environment. Additionally platform or product compatibility may require the application of Epicor or third-party updates, patches and/or service packs and Epicor has no responsibility for compatibility issues which may be caused by updates, patches and/or service packs released by third parties after the date of publication of this document. Epicor® is a registered trademark and/or trademark of Epicor Software Corporation in the United States, certain other countries and/or the EU. All other trademarks mentioned are the property of their respective owners. Copyright © Epicor Software Corporation 2020. All rights reserved. Not for distribution or republication. Information in this document is subject to Epicor license agreement(s).

DOC0091E9

10.2.700

Revision: October 16, 2020 5:49 a.m.

Total pages: 359

sys.ditaval

# Contents

<b>Introduction.....</b>	<b>14</b>
Purpose of this Guide.....	14
Intended Audience.....	14
How Its Organized.....	14
<b>Epicor ERP Architecture.....</b>	<b>16</b>
Epicor N-Tier Model.....	16
Architecture Layers.....	18
Data Flow.....	19
Component Flow.....	20
Report/Process Flow.....	23
Network Protocol Bindings.....	27
Protocols.....	28
Standard HTTP Binding Types.....	28
Transport Encryption Methods.....	29
Serialization.....	29
Compression.....	29
User Authentication.....	29
Protocol Selection.....	30
Binding Options.....	31
UsernameWindowsChannel.....	31
Windows.....	32
UsernameSSLChannel.....	33
HttpBinaryUsernameSslChannel.....	34
HttpsBinaryUsernameChannel.....	35
HttpsBinaryWindowsChannel.....	36
HttpsOffloadBinaryUserNameChannel.....	37
HttpsOffloadBinaryAzureChannel.....	37
HttpsBinaryAzureChannel.....	38
SSL Certificates with Multiple Sites.....	39
Custom Bindings.....	40
Server Binding.....	40
Client Binding.....	40
<b>System Tasks.....</b>	<b>42</b>
Server Security.....	42
Prerequisites.....	42
Administration Account.....	42
Create Account.....	42
Assign Server Roles.....	43
Assign User Mappings.....	44
Database Manager Account.....	45
Create Account.....	45

Create an Application Server.....	46
Prerequisites.....	46
Add Servers.....	46
Application Server Settings.....	47
Database Connection.....	52
Admin Console Settings.....	52
Reporting Services.....	54
Deploy the Server.....	56
Add Extensions.....	58
Install Extensions.....	58
Web Access.....	58
Mobile Access.....	60
Enterprise Search.....	62
Epicor Education.....	64
Information Worker.....	66
Epicor Help.....	68
Data Discovery.....	69
Web Configurator.....	72
Configure Remote Machines.....	74
Remote Connection Setup.....	74
Add a Task Agent.....	74
Remote Firewall Setup.....	75
Launch Task Agent Service Configuration.....	76
Create a New Task Agent.....	76
Windows Endpoint Configuration.....	80
Activate Module Licenses.....	81
Launch Epicor Administration Console.....	81
Import License File.....	81
View and Edit License Properties.....	82
License States.....	82
Delete License.....	83
Update License.....	83
Review Users and Licenses.....	84
Check Active Users.....	84
Check Active Licenses.....	84
Rebuild Indexes.....	85
Create Index Maintenance Plan.....	85
Define Rebuild Index Task.....	86
Finish the Plan.....	87
Regenerate Data Model.....	87
Epicor Administration Console Option.....	88
Launch from Console.....	88
Standalone Launch Options.....	89
Modify the Data Model Generator File.....	89
Modify the Configuration File.....	90

Launch from Command Line.....	90
Launch from Desktop Icon.....	91
Launch as a Recurring Task.....	92
Data Model Customization.....	94
Table Standards.....	94
Included and Excluded Tables.....	94
Include Schemas.....	94
Exclude Tables.....	95
Manual Database Backup.....	96
Run the Backup.....	96
Backup Maintenance Plan.....	97
Create Maintenance Plan.....	98
Check Database Integrity.....	99
Define Full Backup.....	100
Define Differential Backup.....	101
Define Transaction Log Backup.....	101
Finish the Maintenance Plan.....	102
Email Notification.....	103
Restore Database.....	103
Restore from Backup.....	103
Purge Database.....	104
Run the Purge.....	105
Purge Tasks.....	106
Changing Task Agent Purge Settings.....	106
Configure Application Request Routing.....	107
Install and Configure Application Request Routing.....	107
Create Certificates.....	109
Set Up HttpsOffloadBinaryUserNameChannel Server.....	110
Set Up HttpsBinaryUserNameChannel Server.....	111
Configure Application Servers.....	112
Add Certificates.....	113
Add Certificate for Default Website.....	113
Add Self-Signed Certificates (Test Environment).....	113
Manage Load Balance.....	116
Route Specific Calls to Server Farm.....	116
Test Load Balance.....	117
<b>Manage Epicor ERP.....</b>	<b>119</b>
Authentication - User Identity Security.....	119
Epicor Account Authentication.....	120
Password Policy Maintenance.....	120
Define Password Policy.....	120
Expire All Passwords.....	121
Special Characters List.....	122
Password Management.....	122
Password Options.....	122

Account Lockouts.....	123
Account Lockout Policy.....	123
Locked Accounts.....	124
Automatic Sign On.....	126
Allow Automatic Sign On.....	126
Windows Account Authentication.....	127
Password Policy (Windows).....	127
Account Lockout Policy (Windows).....	127
Single Sign-On (Windows Authentication).....	128
Epicor ERP Setup.....	129
Server Configuration.....	130
Administration Console Setup.....	130
Client Configuration.....	131
Azure AD Authentication.....	131
Configure Azure Portal.....	132
Obtain Azure Tenant ID.....	132
Register Server Application.....	133
Register Client Application.....	137
Epicor Administration Console Bindings.....	141
Configure Azure AD Authentication.....	142
Update User File.....	143
Update Client .sysconfig.....	144
Update .sysconfig on Logon.....	145
Login Process.....	146
Optional Server Settings.....	147
Multi-Factor Authentication via Azure AD.....	147
Troubleshooting.....	148
Client Logging.....	148
Server Logging.....	149
Solving Logon Errors.....	149
Epicor Identity.....	150
Authentication Overview.....	151
Obtaining a Token.....	153
Account Self-Service.....	154
Multi-factor authentication.....	155
Multi-factor Authentication Logon Experience.....	156
Documentation Resources.....	160
Authorization - Interface Security.....	161
Security Privileges.....	162
Company Security.....	162
Security Group Maintenance.....	162
Create a Security Group.....	162
User Security.....	163
Security Manager Levels.....	163
Assign Security Privileges.....	163

Assign Security Groups.....	165
Security Logic Hierarchy.....	165
Assign Security.....	166
Run Time Argument Menu Control.....	166
Define Run Time Arguments.....	167
Menu Security.....	167
Create a Security Code.....	168
Assign Menu Security.....	169
Security Group Conflicts.....	169
Service and Method Security.....	170
Assign Service (Business Object) Security.....	170
Assign Method Security.....	171
Field Security.....	172
Assign Global Field Security.....	172
Security Group Field Security.....	173
Security Management.....	173
Change Log Report.....	174
Logon Failure Audit Report.....	174
Menu Security Report.....	174
System Activity Log.....	175
Users/Groups Report.....	175
User Session Log Report.....	175
Configuration Settings File.....	176
File Customization.....	176
ConfigEditor Tool.....	176
Configuration Settings File Functionality.....	177
Default.sysconfig File.....	177
Use the ConfigEditor Tool.....	177
Configuration Settings List.....	178
Application Settings.....	178
User Settings.....	187
Deployment Settings.....	193
Help Settings.....	195
Sort Settings.....	196
Alternate Configuration Settings Files.....	197
Run Time Arguments.....	197
Enter a Run Time Argument.....	198
Run Time Arguments List.....	198
Automatic Schedules.....	200
Create an Automatic Schedule.....	201
Select a Schedule.....	202
Create a Process Set.....	203
Refine and Schedule a Process Set.....	204
Review Tasks.....	204
System Monitor.....	205

Clear Application Cache.....	206
Display the Application Cache.....	206
Clear the Application Cache.....	207
Management Programs.....	207
Conversion Workbench.....	207
Customization/Personalization Maintenance.....	208
Dashboard Maintenance.....	208
Data Fix Workbench.....	209
Data Health Check Workbench.....	209
Data Tag Maintenance.....	209
File Attachment Maintenance.....	210
Personalization Purge.....	210
Query Conversion Maintenance.....	210
System Activity Log Purge.....	211
Updatable Query Maintenance.....	211
<b>Manage Epicor Web Access.....</b>	<b>212</b>
Clear Cache.....	212
Configure Crystal Reports.....	214
Configure Embedded Education.....	214
Configure Enterprise Search.....	215
Configure Help.....	216
Deploy Customizations.....	217
Deploy Dashboards.....	218
License Options.....	219
<b>Multiple Environments.....</b>	<b>220</b>
Self-Signed Certificates - Test Environments.....	220
Determine Setup Process.....	220
Create the Certificate.....	221
Web.Config Setup Process.....	222
Update Web.Config File.....	222
Export the Certificate - Optional.....	223
Import the Certificate - Optional.....	223
Add to Trusted Root Certificates.....	224
Update the Application Server.....	225
HTTPS Setup Process.....	225
Export the Certificate.....	225
Import the Certificate.....	226
Update .sysconfig Files.....	227
Set Binding.....	228
Update the Application Server.....	228
WCF Setup Process.....	229
Export the Certificate.....	229
Import the Certificate.....	230
Update .sysconfig Files.....	230

Move a Database from Production to Test.....	231
Stop Test Application Server.....	231
Backup Live Data.....	231
Update Test Environment.....	233
Clear Source Values - Optional.....	233
Start Test Application Server.....	234
Move Reports Between Environments.....	235
Move with Report Style Maintenance.....	235
Export the Report.....	235
Import the Report.....	236
Move with Solution Workbench.....	237
Create the .CAB File.....	237
Export the Reports.....	238
Import the Reports.....	238
AFR Integration - Restore Database.....	239
Delete AFR Replication Tasks.....	239
Restore from Backup.....	240
Recreate AFR Replication Tasks.....	241
Select Database.....	241
Define Tasks.....	242
Aggregation Types.....	243
Miscellaneous Options.....	243
Complete the Tasks.....	243
<b>Releases and Updates.....</b>	<b>245</b>
Database Migration.....	245
Releases.....	245
Updates.....	246
Method Changes.....	246
Schema Changes.....	246
User Interface Changes.....	247
<b>Logging.....</b>	<b>248</b>
Financial Logs.....	248
Bank Statement Conversation Log.....	248
Bulk Address Validation Log.....	248
Fix BankTran Reporting Amounts Log.....	249
Posting Engine Log.....	249
Recalculate Bank Balances Log.....	250
Recalculate Customer Credit Log.....	250
Release Data Locked for GL Posting Log.....	251
Transfer Balances Log.....	251
UD Codes Creation for Intrastat Log.....	251
Unlock Bank Statement Log.....	252
Unlock Batch Log.....	252
Use Tax Calculation Log.....	252

Verify Balance Records Log.....	253
Integration Logs.....	253
ECC Customer/Consumer Synchronization Log.....	253
ECC Supplier Synchronization Log.....	254
Export to Mattec Log.....	254
Generic Integration Log.....	255
Generic Import Log.....	255
PLM Log.....	256
Manufacturing/Distribution Logs.....	256
Auto Job Closing Log.....	256
Auto Job Completion Log.....	257
Auto Job Firm Log.....	257
Auto Job Release Log.....	258
Backflush Labor Log.....	258
Calculate Global Scheduling Order Log.....	259
Convert PclnValues Log.....	260
Detect Redundant BOMs Log.....	260
Global Scheduling Log.....	261
Import Labor / Scheduling Parameters Log.....	261
Manufacturing Lead Time Calculation Log.....	262
Material Requirements Planning (MRP) Log.....	262
MRP Processor Log Organization.....	263
MRP Scheduler Log Organization.....	265
Abandoned Errors.....	266
Balancing Processors and Schedulers.....	267
Planning Workbench Job Log.....	267
Process MRP Recalculation Needed Log.....	268
Production Yield Recalculation Log.....	268
Refresh PartBin QOH From PartTran Log.....	269
RoHS Job Compliance Log.....	269
RoHS Part Compliance Log.....	269
Multi-Company Logs.....	270
Enterprise Configurator Log.....	270
Enterprise Configurator Direct Log.....	271
Multi-Company Log.....	272
Multi-Company Direct Log.....	272
Multi-Tenant Logs.....	273
ECC Convert Web Customer / Part UOM Log.....	273
Fix Book Detail Records Log.....	274
Fix Book Release Records Log.....	274
Refresh Order Release Quantity Log.....	274
Remove Orphaned PickedOrders / MtlQueue Log.....	275
Program Logs.....	275
Memos.....	275
Fields.....	276

Add a Memo.....	276
Edit a Memo.....	276
Delete a Memo.....	276
Attachments.....	277
Attach a File from the Menu Option.....	277
Attach a File Using Drag and Drop.....	277
Display Attached File.....	278
Remove Attached File.....	278
Audit Logs.....	279
View the Audit Log.....	279
Call Logs.....	279
Call Log Overview Fields.....	280
Make a New Call Log Entry.....	280
Change Logs.....	281
Enable Change Log for a Program.....	281
Review a Change Log.....	282
Transaction Logs.....	283
Review the Transaction Log.....	283
Purchasing Logs.....	283
Generate Purchasing Suggestions Log.....	283
Generate Purchase Schedules Log.....	284
RoHS Supplier Pricelist Compliance Log.....	285
Sales Logs.....	285
Demand Entry Logs.....	285
Demand Header Log.....	286
Detail Fields.....	286
List Fields.....	287
Demand Line Log.....	290
Demand Schedule Log.....	290
Import EDI Demand Log.....	290
Regenerate Configurations Log.....	291
Verify Existing Configurations Log.....	291
System Logs.....	291
Client Tracing Log.....	292
Tracing Options Fields.....	292
Activate From User Account.....	295
Activate From Client.....	297
View the Tracing Log.....	300
Organize the Tracing Log.....	302
Convert the Log Into .xml.....	302
Remove All Tracing Log Entries.....	303
Conversion Log.....	303
Database Migration Log.....	303
Error Message Log.....	304
Global Alert Message Error Log.....	305

Server Log.....	305
Application Server Settings.....	306
System Activity Log.....	309
System Activity Log > Fields.....	309
Activate the Log.....	310
Filter the Data.....	310
Purge Selected Records.....	311
Task Agent Log.....	311
Event Log Viewer.....	311
Event Viewer.....	313
Add Custom View.....	314
Server File Download.....	316
Download a File.....	316
<b>Troubleshooting.....</b>	<b>318</b>
Connectivity Errors.....	318
Load Balancer and Reverse Proxy Connectivity Issues.....	318
Cannot Generate SSPI Context Error.....	319
Insufficient Winsock Resources.....	319
Database Errors.....	320
Create Database Permission Denied.....	320
Database Size Too Small.....	320
Index Outside Bounds of Array.....	321
Wrong Server Data Directory.....	322
Epicor Web Access Errors.....	322
Configurator Error.....	322
Deploy Customization Error.....	323
Invalid User ID.....	324
Logon Errors.....	324
ASP.NET Impersonation Error.....	324
Cannot Log into Modern Shell.....	325
Layer Verification Failure.....	325
Maximum Users Exceeded On License Type.....	326
No License Configured for Company.....	327
Open Exception Error.....	328
Server Rejects Client Credentials.....	329
Printing Outages.....	329
All Reports Have PENDING Status.....	329
Can Preview, Cannot Print.....	330
Cannot Find Report.....	331
Cannot Print to a Client Printer.....	332
CREATE TABLE Permission Error.....	333
LOB Data Exceeds Maximum.....	333
Logon Fails for Execution Account.....	334
Permissions Granted Error.....	335
Printer Setting No Printing Error.....	336

Print Process Times Out.....	336
Remote Name Does Not Resolve.....	337
Server Printing Fails; No Error.....	337
SSRS Style Does Not Display.....	338
Support Checklist.....	339
Eliminate Potential Sources.....	340
Check Customizations.....	341
Disable BPM Directives.....	341
Recompile BPM Directives.....	342
Identify Program.....	343
Main Details.....	343
Save Error Message Log.....	343
Issue Details.....	344
Record Steps to Duplicate.....	345
Gather System Data.....	346
System Information.....	346
Application Server Information.....	346
Configuration Files.....	347
Task Agent and Setup Data.....	347
Event Viewer Files.....	348
Gather Application Data.....	348
Generate Client Logs.....	348
Generate Server Logs.....	349
Capture Logs.....	351
Send the Data.....	351
Performance and Diagnostic Tool.....	352
Verify SSL Certificate Friendly Name.....	353

# Introduction

---

## Purpose of this Guide

---

The System Administration Guide contains the information administrators need to manage both SQL Server and the Epicor ERP application. Use this information to complete system tasks, administrate the application, and troubleshoot issues.

This guide is intended to be your primary resource for maintaining the application. It contains server based information such as adding application servers and setting up regular database backup schedules. The guide explores the tools available within Epicor ERP you can use to define client startup settings, set up single sign on for users, and add automatic schedules that regularly run processes and reports. It also details set up tips for the Epicor Web Access (EWA) browser-based interface.

This guide then explores how you manage the various environments used by your organization for testing software updates and creating custom SSRS reports. Use this information to learn how to move data and reports between your different environments. This guide also contains a list of the logs you can activate to review how specific processes run in the Epicor ERP application.

To complete this user guide, Epicor Technical Support has identified common system issues and their solutions, and these items are documented in the Troubleshooting section. The System Administration Guide concludes with a section on the files and logs you should prepare before you call Epicor Technical Support or seek assistance from your consultant.



**Important** This version of the System Administration Guide is for use with Epicor ERP version 10.1 or higher.

## Intended Audience

---

The guide is intended for system administrators, technical consultants, and partners. The System Administration Guide helps ensure the Epicor ERP application performs as expected and provides guidance on administration areas that should be addressed before contacting Epicor consultants or Epicor Technical Support.

Individuals who perform all or some of these tasks will benefit from reviewing the System Administration Guide.

## How Its Organized

---

This guide is organized by first exploring the typical SQL server tasks you need to run. It then goes into increasing detail about the tools and logs available in the Epicor ERP application, concluding with a Troubleshooting section.

Sections in this guide:

- **Epicor ERP Architecture** - Contains an illustrated overview of how the Epicor ERP application is structured. Use this information to better understand how the Epicor ERP application interacts externally with SQL Server and internally with its databases.

- **System Tasks** - Details administration tasks you need to perform in both SQL Server Management Studio and the Epicor Administration Console. It documents how to create additional application servers, activate module licenses, and back up databases.
- **Manage Epicor ERP** - Explores the various administrative tools and features available within the Epicor ERP application. Leverage these tools to improve how users interact with Epicor ERP.
- **Manage Epicor Web Access (EWA)** - Documents how to configure the EWA interface to display different interface styles, Epicor Education courses, and the application help. It also explores how to deploy custom programs for display on the EWA interface.
- **Multiple Environments** - Contains information about how you move databases and reports between your Epicor ERP environments. By following this documentation, you can move items between Test, Pilot, Live, and any other environments at your organization.
- **Updates** - Describes the installation process you follow when an update becomes available. It also links you with the update installation guide you need on the EPICWeb site.
- **Logging** - This section documents the logs you can run to evaluate Epicor ERP processes. You use these logs to check for errors and evaluate process performance.
- **Troubleshooting** - Review this section to find specific solutions to issues such as printing problems, database errors, and logon errors. It concludes with a Support Checklist that documents the files and logs you gather before you contact your consultant or Epicor Technical Support.

# Epicor ERP Architecture

The Epicor ERP application interacts with databases by using SQL Server. This section of the guide illustrates how the architecture of the application receives user input to update the database and returns the resulting output for display.

By understanding how the Epicor ERP application is designed, you can better interpret the system messages the application sends you and more quickly resolve issues.

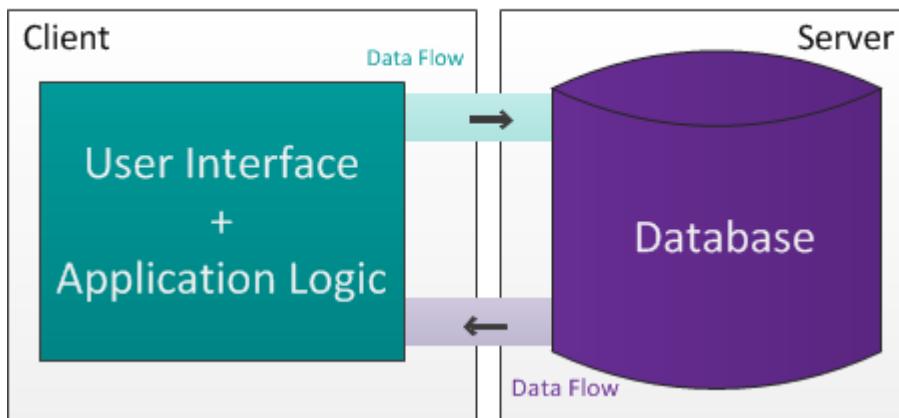
## Epicor N-Tier Model

The Epicor ERP application is a **Microsoft® SQL Server®** environment that uses an n-tier configuration for its database architecture. This configuration offers significant deployment flexibility over both two-tier and three-tier configurations.

### The Two-Tier Model

Traditional client/server development is based on a logical and physical two-tier computing model. This architecture is deployed across two machines connected through a network. The user interface and application logic are tightly integrated and located on a client machine, while the data resides on a separate server machine.

### 2-Tier Model



The major disadvantage to this model is all updates must be run individually on each client machine. Any issues that occur must also be resolved individually on each client machine, making both installation and update tasks a cumbersome process.

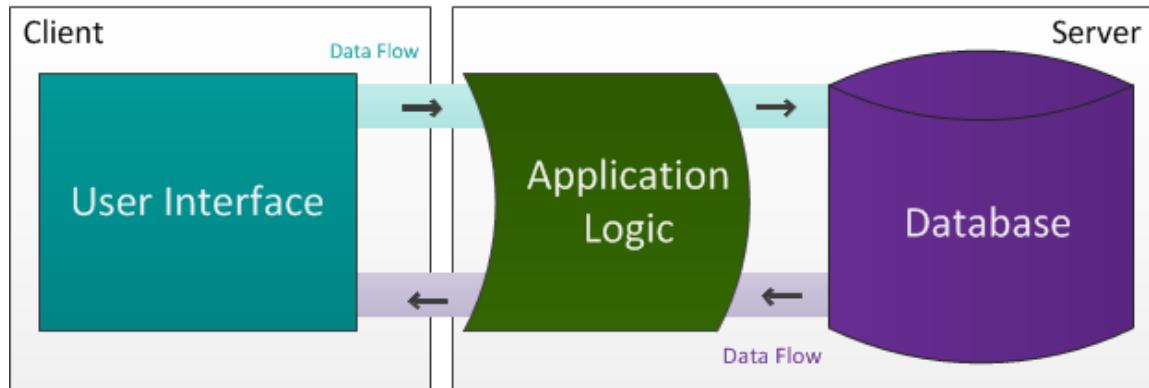
### The Three-Tier Model

The logical three-tier model has a user interface on a machine physically separate from another machine which contains the application logic and the data. Only two machines are physically involved in the hierarchy, but technically, or logically, the architecture has three tiers:

1. User Interface
2. Application Logic

### 3. Database

#### 3-Tier Model

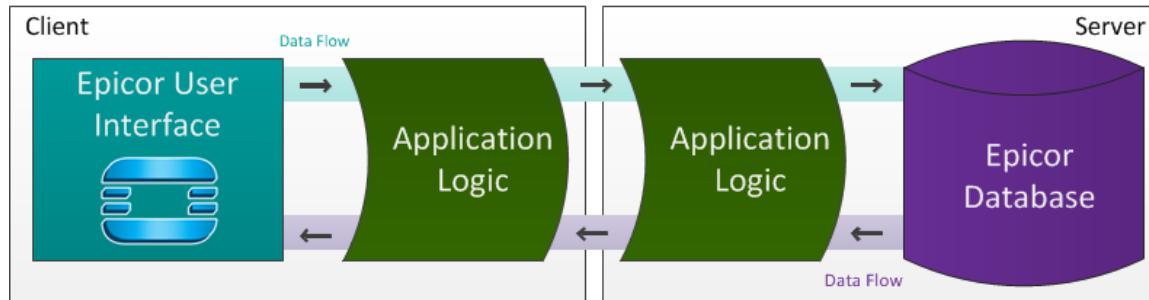


Because the logic for the application is handled through the server, you have more control over updating the application and correcting issues that occur. These changes run on the server and the application logic flows out to the client machines.

#### The N-Tier Model

The Epicor ERP environment supports an n-tier configuration, which means the application logic can be placed in multiple locations between the user interface and the database. This configuration adds deployment flexibility, as you can set a number of logical routines that run before the data reaches the server. The n-tier configuration also has the same advantage as the three-tier configuration; you can update the application from the server.

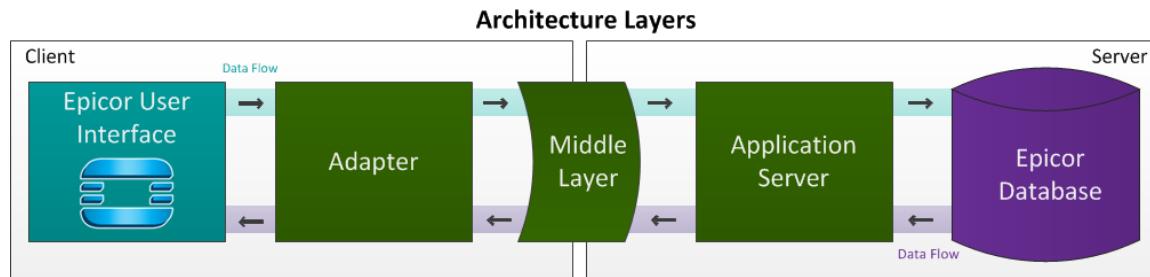
#### N-Tier Model



Although this model does not capitalize on the use of shared memory and introduces an additional network connection you do not have in the logical three-tier model, the deployment flexibility of this model has significant benefits for managing enterprise processes.

## Architecture Layers

Through using the n-tier structure, the Epicor ERP application uses the following architecture layers to create and save data to the database.



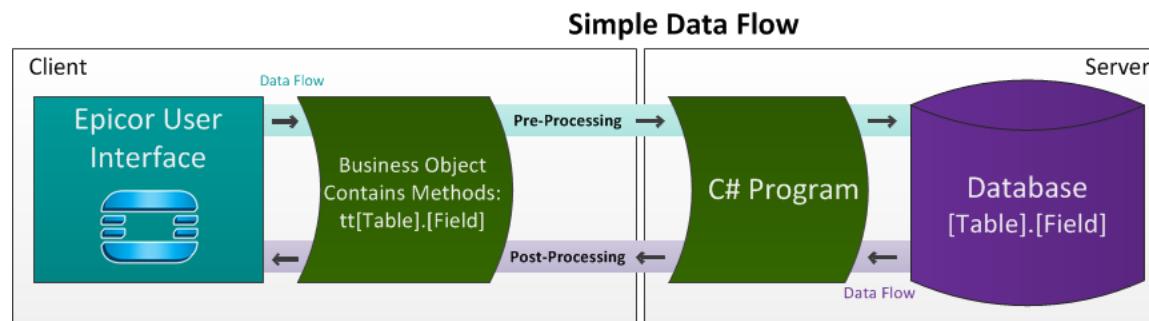
Information about each architecture level:

- **User Interface (UI)** - The user interface layer contains the program windows that display for the end user.
- **Adapter** - The adapter typically defines how the service (business object) manipulates the data both before and after a call. The adapter file is placed in the client directory. It processes the transaction between the user interface and the service (business object) that runs a specific method on the program.
- **Middle Layer** - This layer handles the communication between the client and the server. The Epicor ERP application uses Windows Communication Foundation (WCF) for this layer; the WCF contracts reside on both the client and the server to facilitate this communication.
- **Application Server** - The application server handles the processing through an Internet Information Services (IIS) application pool. The IIS application pool is the process that hosts the application logic; it defines a group of related URLs that use the same process or set of processes. Up to three application servers can run against a specific database.
- **Epicor Database** - The physical database contains the tables/columns that store the data entered and updated by end users.

## Data Flow

When users enter data, the Epicor ERP application moves the data through the architecture layers. This topic details how data flows from the user interface out to the database and back again for display.

The following illustration shows the main transactions that run between the user interface and the database.

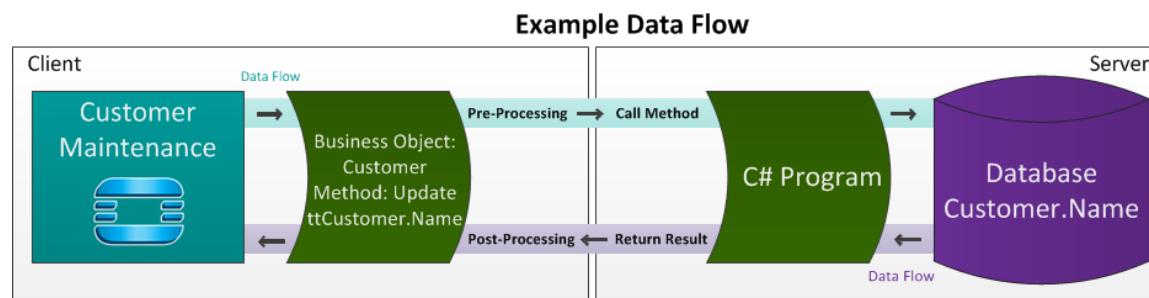


Whenever a user adds, edits, or deletes a record, the Epicor ERP application activates a method inside a business object to handle the transaction. A business object contains a series of methods that control how the user interface connects with specific tables in the database. For example, the Customer business object contains the New, Update, Delete, and other methods that run the changes users make to the Customer table. Notice these methods initially store data in active memory through a series of temporary tables (tt) tables that mirror both the table name and the field name which store the data in the physical database.

The data first goes through a Pre-Processing stage where the new or updated data moves to the database. Users can optionally create Business Process Management (BPM) directives that monitor this data before the method saves the data. A C# program on SQL Server then receives the incoming database changes and sends them to the database.

Once the updated data is saved, the C# program on the server next passes this data back to the method through a Post-Processing stage. Like the Pre-Processing stage, users can optionally create BPM directives that monitor the saved data results. Once again the data flows through the method and displays on the user interface.

The next illustration shows you a specific example of what happens when a user updates the **Name** field on an existing customer record.

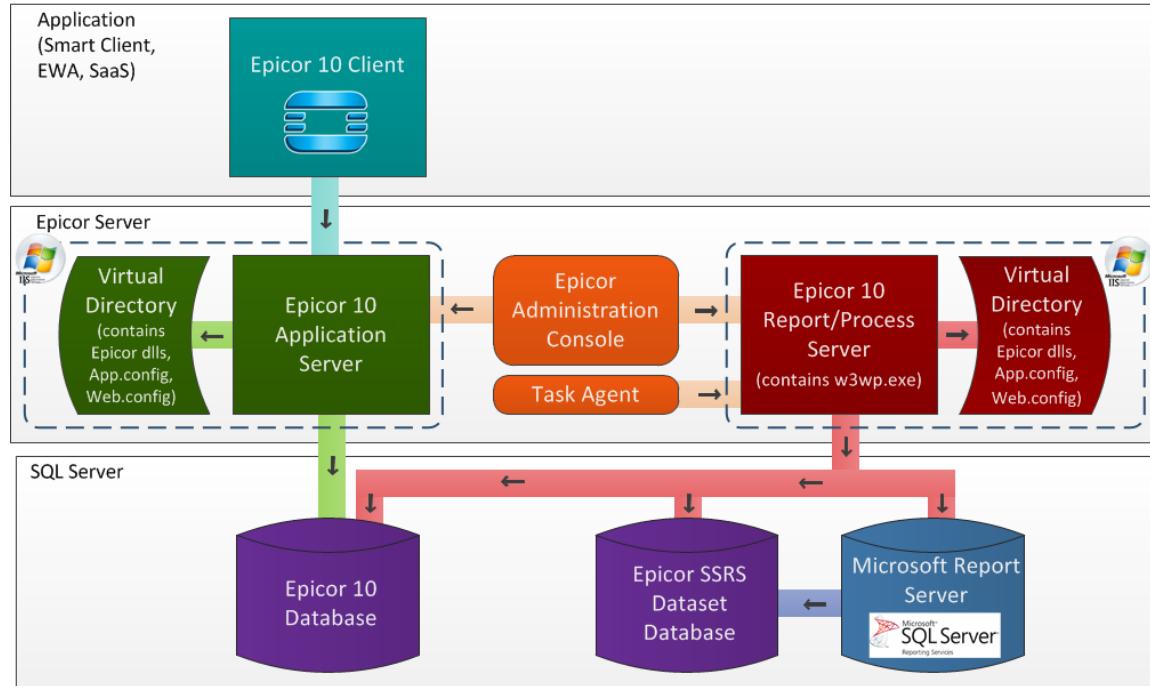


Notice the Update Customer method connects with the C# Code on the server layer. The updated customer record is saved to the physical database, and the resulting data returns for display on the user interface.

## Component Flow

The Epicor ERP application contains a series of primary components that work together as users add and update data. The following diagram illustrates how these components interact while the Epicor ERP application runs.

Notice this diagram expands on the concepts described previously. The Epicor ERP application has a **client layer** that users access to enter database transactions. To update the database, the application has a middle layer comprised of an application server, task agent, report/process server, and virtual directories. Then the database layer contains your physical Epicor database and the SSRS databases required for generating reports.



### Epicor Client

The **Epicor ERP Client** is the visual representation of the application presented to end users. After logging into the application, the user interface displays. The user then launches Epicor ERP programs and enters/updates data. For each program, a business object is underneath the user interface layer. The business object contains the methods that interact with the database like GetNew, GetList, Update, Delete, and so on. When the user clicks interface buttons such as New or Save, the corresponding method activates and sends the data to the **Application Server**.

### Application Server

An **Application Server** manages a specific instance of the Epicor ERP application. Through each application server, you can configure licenses, companies, sessions, and users for a specific database. Each application server resides in the middle layer of the application. After you finish configuring the application server, it then handles the business logic, determining how the incoming data interacts with the Epicor database and then displays on the end user interface.

Each application server interacts with a **Virtual Directory**. This directory is an alias for a physical directory that contains the **Dynamic Link Libraries** (.dll files); these .dll files handle database transactions in the middle layer logic. The Virtual Directory also has the configuration settings files that define various application and server parameters for the Epicor ERP application.

Each application server is also contained within an **Epicor Server**. You create these servers within the **Epicor Administration Console**. (This component is described later in this section.) Each Epicor Server can manage up to three application servers, and these three application servers interact with the same database. Likewise, the Epicor Server interacts with **Internet Information Services (IIS)**. This service is a group of Internet servers that have extended capabilities to handle **Microsoft Windows Server** operating systems. By utilizing IIS, each application server can then interact with the Epicor ERP database.

 **Tip** You learn how to add application servers later in this guide. Review the [Create an Application Server](#) section.

### Report/Process Server

A **Report/Process Server** stores the metadata and object definitions required to generate reports and run database processes. Each report/process server uses the SQL Server Database Engine to store and manipulate data. Whenever a user runs a report or process, the report/process server handles the transaction, populating the **Epicor SSRS Dataset Database** with selected data for the report or process. It also activates the report or process definition controlled by the **Microsoft Report Server**. The report/process server can then either generate the data or build the report.

Like application servers, each report/process server interacts with a **Virtual Directory**. This directory is an alias for a physical directory that contains the **Dynamic Link Libraries**(.dll files); these .dll files handle database transactions in the middle layer logic. The Virtual Directory also has the configuration settings files that define various application and server parameters for the Epicor ERP application.

Additionally each report/process server interacts with a **Virtual Directory** that contains the .dll files and .config files for the Epicor ERP application. Similarly **Internet Information Services (IIS)** contains both the report/process server and the virtual directory; IIS controls how the report/process server interacts with both the **Epicor SSRS Dataset Database** and the **Microsoft Report Server**.

### Task Agent

Task agents handle all scheduled tasks within the Epicor ERP application. The task agent activates any program added to a recurring schedule. Users add programs to recurring schedules through the **Schedule** drop-down lists available on programs throughout the Epicor ERP application. Each task agent runs against a specific database.

Like application servers, you can configure up to three instances of the task agent service to run against a specific database. Each task agent can then run on a local machine or a remote machine. After you set up an application server (AppServer), you can then configure the local or remote task agent for the database.

 **Tip** You learn how to add task agents later in this guide. Review the [Add a Task Agent](#) section.

### Epicor Administration Console

The **Epicor Administration Console** is a separate management utility installed on the server. You use the Epicor Administration Console to manage the Epicor ERP application, creating application servers, databases, and Enterprise Search servers. You can also create and update task agents through this management utility. As illustrated in the previous diagram, the Epicor Administration Console interacts with both the **Application Server** and the **Report/Process Server**. Through this management utility, you can administrate key areas of the Epicor ERP application.

### Epicor 10 Database

The **Epicor 10 Database** is the physical disk that contains your data. As users and modify data, the **Application Server** writes these data changes to the tables in the database. The **Report/Process Server** also interacts with the database, using queries to pull data for generating processes and building reports. You need to regularly back up your database, so be sure to set up this task on a recurring schedule. You also need to perform other tasks to ensure your database contains current data that users can retrieve without errors.



**Tip** These tasks are described later in this guide. Review the **Regenerate Data Model**, **Manual Database Backup**, **Backup Maintenance Plan**, **Restore Database**, and **Purge Database** sections for more information.

## Microsoft Report Server

The **Microsoft Report Server** is a service that handles the data processing, report rendering, and data delivery tasks for SQL Server Reporting Services (SSRS). When the Report/Process Server activates a report/process and sends the data, the Microsoft Report Server uses the report data definition and/or process definition to generate the data or build the report output.

## Epicor SSRS Dataset Database

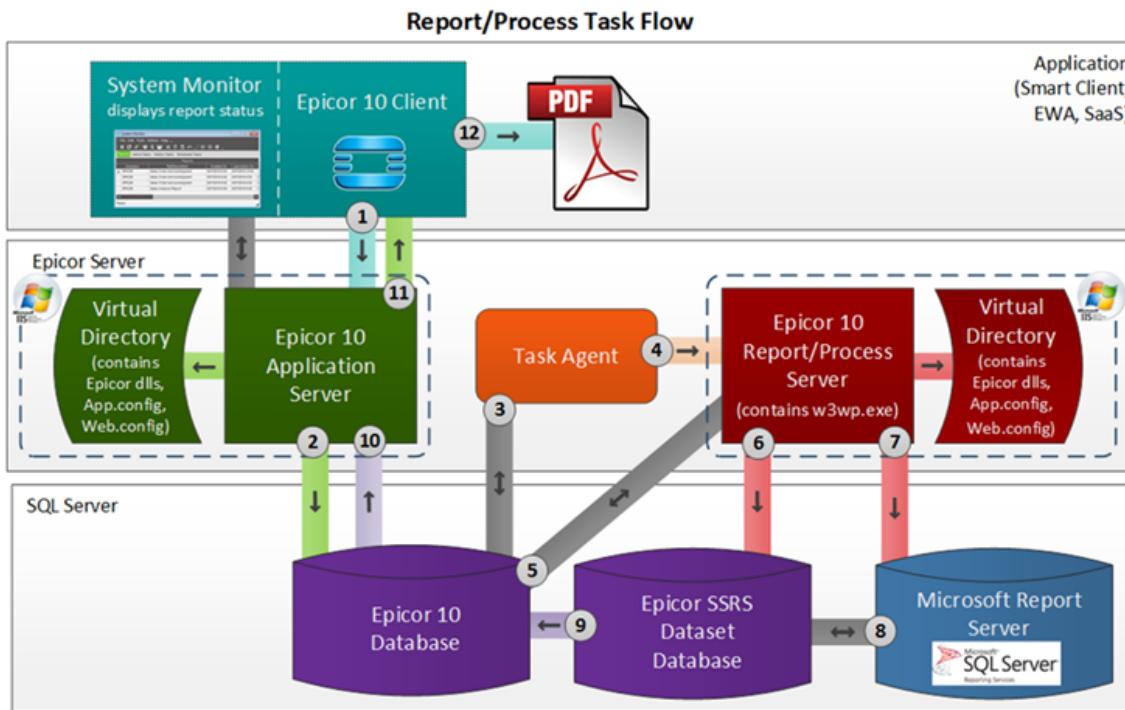
The Epicor ERP application interacts with **SQL Server Reporting Services** (SSRS) to render reports. Each report must contain a dataset that holds the data pulled by a query from the **Epicor 10 Database**. The dataset consists of a query, a collection of data, parameters, filters, and other data options. This dataset defines the data that displays on the rendered report.

## Report/Process Flow

The Component Flow diagram illustrates how the various components of the Epicor ERP application interact. This next diagram now examines these components in more detail by showing how a report or process moves through these various components.

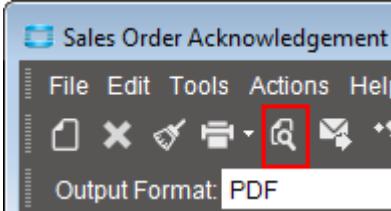
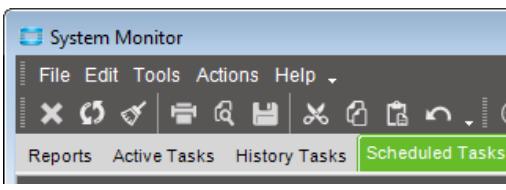
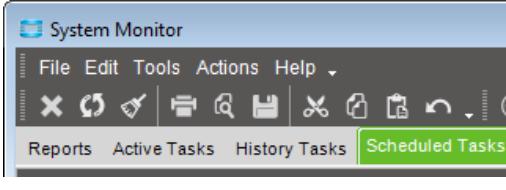
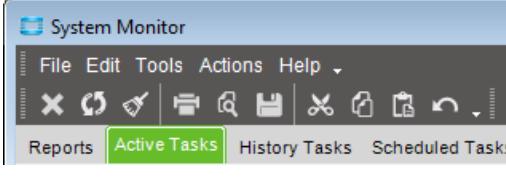
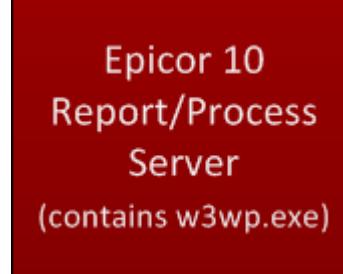
Notice each component interaction in the report/process flow is numbered. Use the table below the diagram to review how each component interacts with the next component in the flow. The table uses a specific example, the Sales Order Acknowledgment report, to explain how reports render for preview or print. Processes follow a similar flow through these Epicor ERP components, but they primarily update records in the Epicor ERP database. Through the report flow, the final report output either generates for display or print.

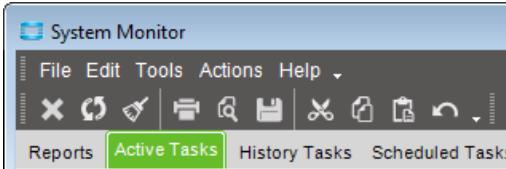
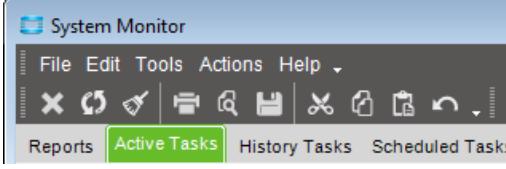
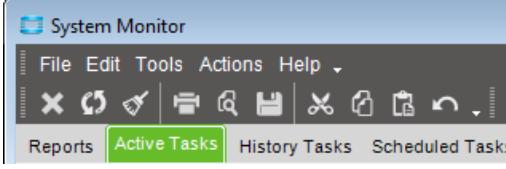
This diagram also includes the **System Monitor**. A user can launch this program to check on the current status of the report. While the report process generates the preview for the Sales Order Acknowledgment, the System Monitor constantly checks the status of the report/process task. It does this by repeatedly running the **GetRowsKeepIdleTime()** method to check for activity. When the System Monitor discovers a method has run, it updates the status of the report on its various tasks. When the report finishes generating, the System Monitor returns the **SysRptLst** table which displays a list of the finished reports.

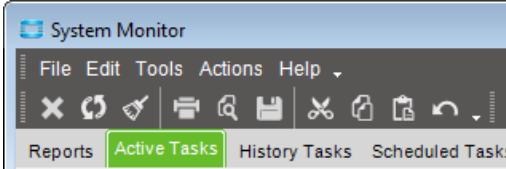
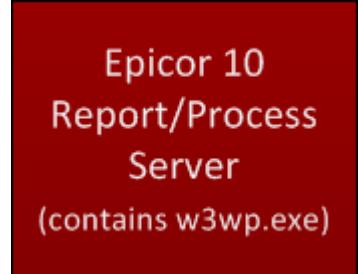
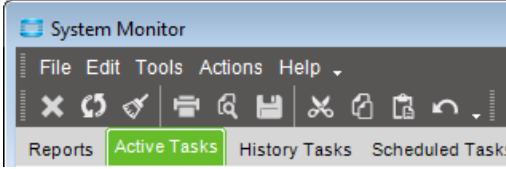
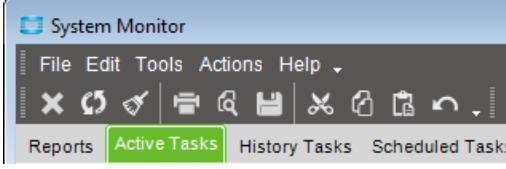
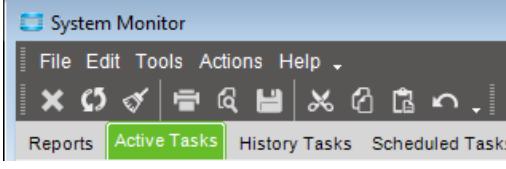


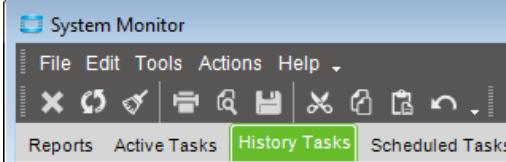
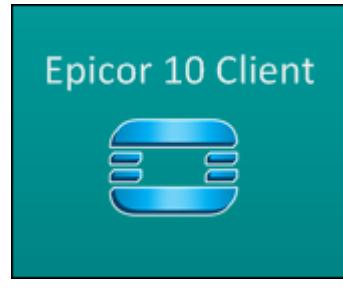
### Report Flow Step by Step

The following table describes each step within the report/process task flow. It does this by first describing what you see on the user interface, and then details the task action each component launches in the process flow.

What You See	Task Action
 <p>You want to review the current sales order in the Print Preview window. Within <b>Sales Order Entry</b>, you click <b>Actions &gt; Print Sales Order Acknowledgment</b>. You then click the <b>Print Preview</b> button.</p>	 <p>1. The <b>Epicor 10 Client</b> component calls the <b>SalesOrderAck.SubmitToAgent</b> method (API). This launches the Print Preview task on the <b>Epicor 10 Application Server</b>.</p>
 <p>The System Monitor displays the Print Preview task on the <b>Scheduled Tasks</b> tab. If the task remains on this tab for a long time, it means the Task Agent has not yet picked up the task. This could indicate either the task or Task Agent itself has a problem.</p>	 <p>2. On the <b>Epicor 10 Application Server</b>, the <b>SubmitToAgent</b> method inserts data into the <b>Epicor 10 Database</b> for the sales order Print Preview task. This information is placed in the <b>ICE.SysAgentSched</b>, <b>ICE.SysAgentTask</b>, and <b>ICE.SysAgentTaskParam</b> tables. These tables store the sales order number, user, and other details. These details are required to render the sales order preview.</p>
 <p>The System Monitor displays this task on the <b>Scheduled Tasks</b> tab.</p>	 <p>3. The <b>Task Agent</b> constantly reads the <b>ICE.SysAgentSched</b>, <b>ICE.SysAgentTask</b>, and <b>ICE.SysAgentTaskParam</b> tables. When it finds the Print Preview task, it picks up the report / process and inserts an <b>ICE.SysAgentTask</b> and <b>ICE.SysAgentTaskParam</b> record into the Sales Order Acknowledgment report.</p>
 <p>When the report is launched by the <b>Task Agent</b> on the <b>Epicor 10 Report / Process Server</b>, the System Monitor now displays this task on the <b>Active Tasks</b> tab.</p>	 <p>4. The <b>Task Agent</b> launches the Print Preview task on the <b>Epicor 10 Report/Process Server</b>.</p>

What You See	Task Action
	<p>Notice the Task Agent only launches the Print Preview task on the Epicor 10 Report/Process Server; it does not run it.</p> <p>The Task Agent also does not need to run on a server with a lot of resources, but the Epicor 10 Report / Process Server must have enough resources (correctly sized) to handle report and process tasks.</p>
 <p>The System Monitor continues to display this task on the <b>Active Tasks</b> tab.</p> <p>You can view the progress of the Print Preview task by navigating to the <b>Active &gt; Detail and Active &gt; Logs</b> sub sheets. If you suspect performance is slow, you can use this log to determine which tasks are taking longer to complete.</p>	<p><b>Epicor 10 Report/Process Server</b> (contains w3wp.exe)</p> <p>5. The <b>Epicor 10 Report/Process Server</b> now runs the business logic for the Print Preview task, pulling the sales order data from the <b>Epicor 10 Database</b> and executing the business logic for the Sales Order Acknowledgment report.</p> <p>Note this task runs on the machine that contains the <b>Epicor 10 Application Server</b> or the <b>Epicor 10 Report/Process Server</b>, and not the machine that contains the <b>Task Agent</b>.</p> <p>If you have a dedicated print/background process application server, the Print Preview task runs on this separate <b>Epicor 10 Report/Process Server</b>.</p>
 <p>The System Monitor continues to display this task on the <b>Active Tasks</b> tab.</p>	<p><b>Epicor 10 Report/Process Server</b> (contains w3wp.exe)</p> <p>6. When the business logic for the Print Preview task finishes running on the <b>Epicor 10 Report/Process Server</b>, the ICE Framework writes the report data to the <b>Epicor SSRS Dataset Database</b>.</p> <p>Because the Print Preview task is generating a Sales Order Acknowledgment, the <b>OrderHed</b>, <b>OrderDtl</b>, <b>OrderRel</b>, and other tables are created in the <b>Epicor SSRS Dataset Database</b>. These tables only display information from the selected sales order.</p>

What You See	Task Action
 <p>The <b>System Monitor</b> continues to display this task on the <b>Active Tasks</b> tab.</p>	 <p><b>Epicor 10 Report/Process Server</b> (contains w3wp.exe)</p> <p>7. Now through the Sales Order Acknowledgment business logic, the <b>Epicor 10 Report/ Process Server</b> invokes the <b>Microsoft Report Server (SSRS)</b>.</p>
 <p>The <b>System Monitor</b> continues to display this task on the <b>Active Tasks</b> tab.</p>	 <p><b>Microsoft Report Server</b> Microsoft SQL Server Reporting Services</p> <p>8. <b>Microsoft Report Server</b> reads the Sales Order Acknowledgment data from the <b>Epicor SSRS Dataset Database</b> and then renders the data in the .pdf file format.</p>
 <p>The <b>System Monitor</b> continues to display this task on the <b>Active Tasks</b> tab.</p>	 <p><b>Epicor SSRS Dataset Database</b></p> <p>9. The ICE Framework inserts the rendered .pdf binary data from the <b>Epicor SSRS Dataset Database</b> into the <b>ICE.SysRptLst</b> table within the <b>Epicor 10 Database</b>.</p>
 <p>The <b>System Monitor</b> continues to display this task on the <b>Active Tasks</b> tab.</p>	 <p><b>Epicor 10 Application Server</b></p> <p>10. The <b>Epicor 10 Application Server</b> constantly runs the <b>ReportMonitor.GetRowsKeepIdleTime()</b> method to check on the current state of the <b>Epicor 10 Database</b>. When the Print Preview task is complete, this method returns report data to the <b>ICE.SysRptLst</b> table.</p>

What You See	Task Action
	<p>You can set how often the <b>GetRowsKeepIdleTime()</b> method runs within the <b>System Monitor</b>. To do this, launch the <b>Actions &gt; Configurations</b> window.</p>
 <p>The <b>System Monitor</b> now displays this task on the <b>History Tasks</b> tab.</p> <p>This task remains on this tab for the length of time defined on the <b>Archive Period</b> on the report. If you need, use the History Tasks tab to preview or print this report again.</p>	 <p><b>11.</b> The <b>Epicor 10 Client</b> retrieves the .pdf binary data. It does this by calling the <b>SysMonitorTasks.GetRows</b> method.</p>
 <p>The <b>Epicor 10 Client</b> then renders the <b>Sales Order Acknowledgment</b> in the <b>Print Preview</b> window.</p> <p>To display the report in the Print Preview window, the <b>PDF Viewer</b> must be installed on the client.</p>	 <p><b>12.</b> The <b>Epicor 10 Client</b> now calls the <b>PDF Viewer</b> to display the report in the <b>Print Preview</b> window.</p> <p>If the report file contains a large amount of data, it can take longer to render the report.</p>

## Network Protocol Bindings

The Windows Communication Foundation (WCF) hosts the services for your Epicor application.

By working with the Epicor ICE Framework, the Windows Communication Foundation manages the service calls, or messages, that users initiate on clients. These messages are then transported to the server, where application code updates the database. Together both the Epicor ICE Framework and the WCF form a secure and efficient pipeline that sends the service call messages between the clients and servers across your network.

You can use different WCF protocol bindings to facilitate this network communication. The Epicor application utilizes several binding options, so you need to select the protocol binding that best matches the transport of different functions. If you have an environment integrated with Service Connect, generate reports on a separate server, or require a similar processing need, you can set up multiple application servers to update the same

database. Each application server can have a different protocol binding that best facilitates the configuration it needs to execute its function. Utilizing multiple application servers can also help you load balance the demand on your network.

This section first describes the main aspects of network protocols to help you understand the differences between them. Then this section details each protocol binding option you can activate for the Epicor application. By reviewing this information, you will be better able to determine which protocol binding to select and implement.

## Protocols

The Epicor application supports NET.TCP, HTTP, and HTTPS protocols.

### NET.TCP

NET.TCP is designed to facilitate communication between servers that reside in the same data center. For example, the Epicor task agent schedules tasks within its application server and so the NET.TCP protocol bindings can handle this network communication.

However this protocol does not work as well over the internet. Because the NET.TCP protocol needs to keep communication constantly open between the clients and servers, firewalls and routers can disrupt the transport pipeline. These bindings are faster than the available HTTP binding, but you can only use them for WCF to WCF communication.

### HTTP

The Epicor application uses Hypertext Transfer Protocol (HTTP) to support data communication through the Simple Object Access Protocol 1.2 (SOAP). Through SOAP the data message is encrypted, but the transport process for this data is not encrypted. To do this, HTTP uses the WSHttpBinding. This binding is similar to the BasicHttpBinding, but it provides message security, transaction, consistent messages, and WS Addresses.

Epicor supports the HttpBinaryUserNameSslChannel binding option. This binding encrypts the body of the message. It does not use Hypertext Transfer Protocol Secure (HTTPS), so it tends to be slower than bindings which use HTTPS.

### HTTPS

The Hypertext Transfer Protocol Secure (HTTPS) bindings are designed to facilitate communication between clients across Wide Area Networks (WANs) and the internet. These protocols can also handle communication within Local Area Networks (LANs), but a purchased or self-signing certificate is required to maintain the integrity of the system.

If you need to set up an application server that communicates with components over the internet, you should select one of the HTTPS protocol bindings.

## Standard HTTP Binding Types

The following HTTP binding types are pre-defined in Windows Communication Foundation (WCF). These binding types are only used with the HTTP and HTTPS protocols.

### basicHttpBinding

This binding exposes endpoints that communicate through ASMX based Web services and other services that conform to the WS-I Basic Profile 1.1. The transport of messages is secured through HTTPS.

### wshttpBinding

This binding uses WS-Reliable Messaging for reliability and WS-Security for message security and authentication. Message transport is handled by HTTP and is not encrypted, but the messages themselves are encoded using Text/XML.

### webHttpBinding

Instead of using SOAP requests, the webHttpBinding exposes the communication endpoints through HTTP requests. These endpoints are used for REST integration within the Epicor application. The transport of messages is secured through HTTPS.

## Transport Encryption Methods

When the protocol binding encrypts the network transport process, it uses the following methods:

- **Windows** - If the client and server use the same Windows Domain, WCF can leverage the domain to secure the network transport. Either the client and the server must be on the same Windows Domain, or the client and server domains need to have a trust relationship between different domains.
- **Secure Sockets Layer (SSL)** - If the client and the server are on separate, untrusted Windows Domains or do not reside on any domain, the Secure Sockets Layer (SSL) is used to encrypt the network transport. The client and server machines must trust the authority that issues the certificate. You typically do this by obtaining a certificate from Verisign or a similar Microsoft approved authority. Your IT organization can also issue and manage internal certificates.

## Serialization

When a user enters data on a form and sends it across the network to the server, this data is transformed from the object behind the form into a variety of formats that allow data to be sent across networks. These formats include binary, JSON, and XML.

The Epicor application can do this transformation, or serialization, through the following methods.

- **Custom Binary** -- The Epicor application can utilize a custom binary serialization optimized for performance. This serialization is used when the Epicor application code runs on both the client and the server. The data format is designed for effective network performance. However Custom Binary serialization is difficult to integrate with other applications. You cannot use custom binary serialization if your client runs on a non-Windows platform such as Linux or another operating system.
- **Interoperability** -- When the client does not use .NET or Epicor code, the Epicor application uses the .NET Data Contract Serializer. Both the SOAP 1.1 and 1.2 can then be available to transport the XML data over the network. The REST endpoints also support both XML and JSON.

## Compression

The network protocols available in the Epicor application all support data compression.

## User Authentication

You can secure user identities through either Windows domain credentials or Epicor user account credentials. If you use Windows credentials, the transport encryption type used by the protocol binding affects how user identities are secured within the Windows domain.

## Protocol Selection

The following table summarizes the main differences between each protocol.

	<b>Latency</b>	<b>Wire Efficiency</b>	<b>Cloud Reliability</b>	<b>Interop</b>	<b>Load Balancing</b>	<b>Privacy</b>	<b>Comment</b>
NET.TCP	Best	Very Good	Good	None	Requires Hardware and Server Affinity	Windows, SSL	Default for on-premise servers
HTTPS/Binary	Very Good	Very Good	Very Good	None	Easiest to Configure	SSL	Best for cloud or VPM infrastructures
HTTP/SOAP 1.2	Acceptable	Very Good	Very Good	Good	Easiest to Configure	WS-SecureConversation	Best for WS* Configurations
HTTPS/SOAP 1.1	Good	Good	Good	Good	Easiest to Configure	SSL	Needed for non-WS* clients like Ruby and Python

## Binding Options

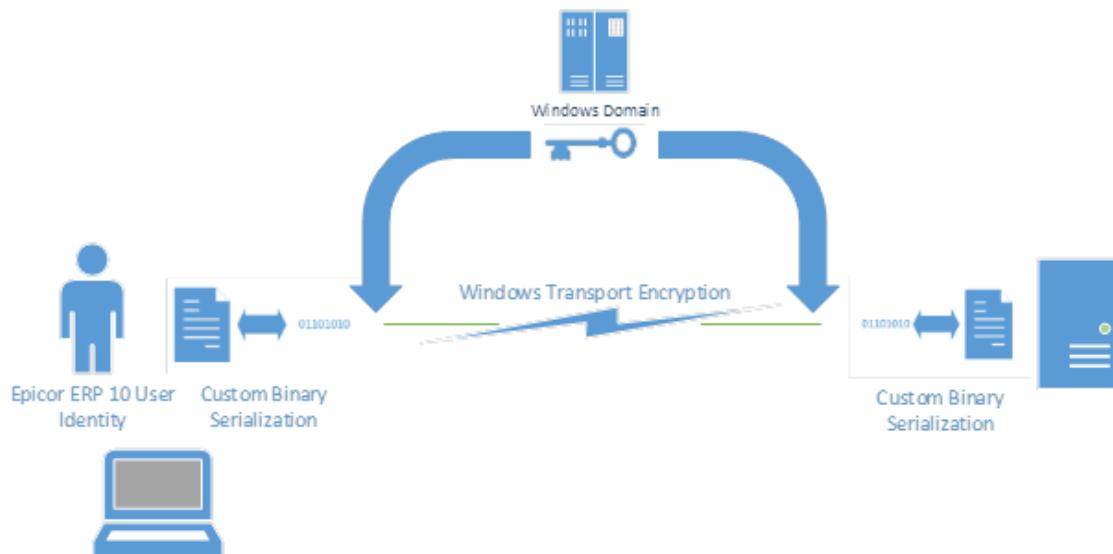
The Windows Communication Foundation (WCF) has several protocol binding options. Most of the WCF binding options available for your Epicor application are custom bindings optimized for specific environments.

This section documents each protocol binding available within the Epicor application.

### UsernameWindowsChannel

This NET.TCP binding authenticates transactions through an Epicor Username and Password. Windows checks for existing Epicor user accounts to authenticate logins.

The following diagram illustrates how this binding handles network transactions.



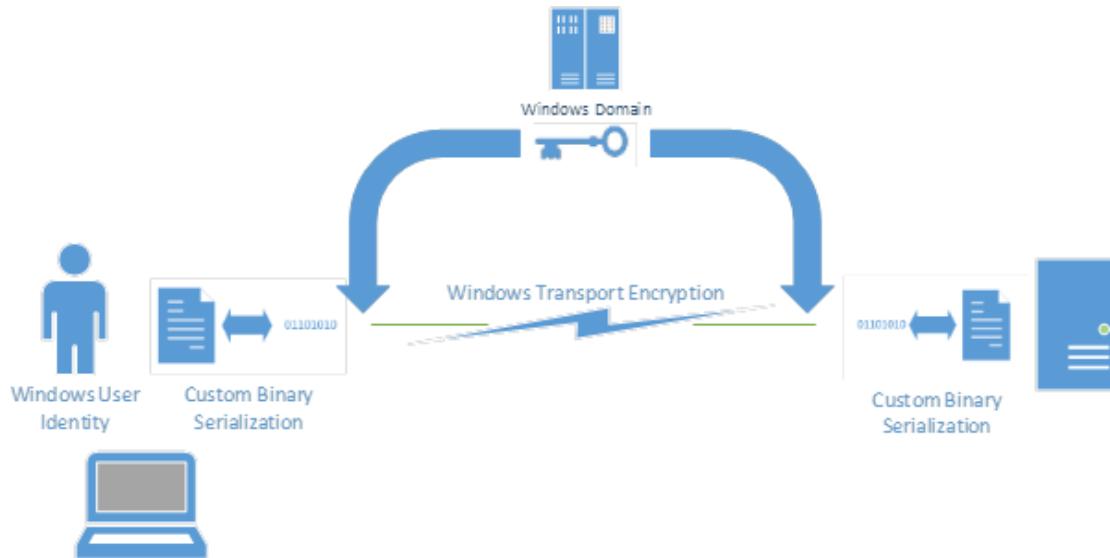
Protocol binding features:

- Epicor user account (User ID/Password) token required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The serialized data is compressed through a custom routine developed by Epicor.
- Windows encrypts the transport between the client and the server.

## Windows

This NET.TCP binding authenticates transactions using a Windows Username and Password. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.

The following diagram illustrates how this binding handles network transactions.



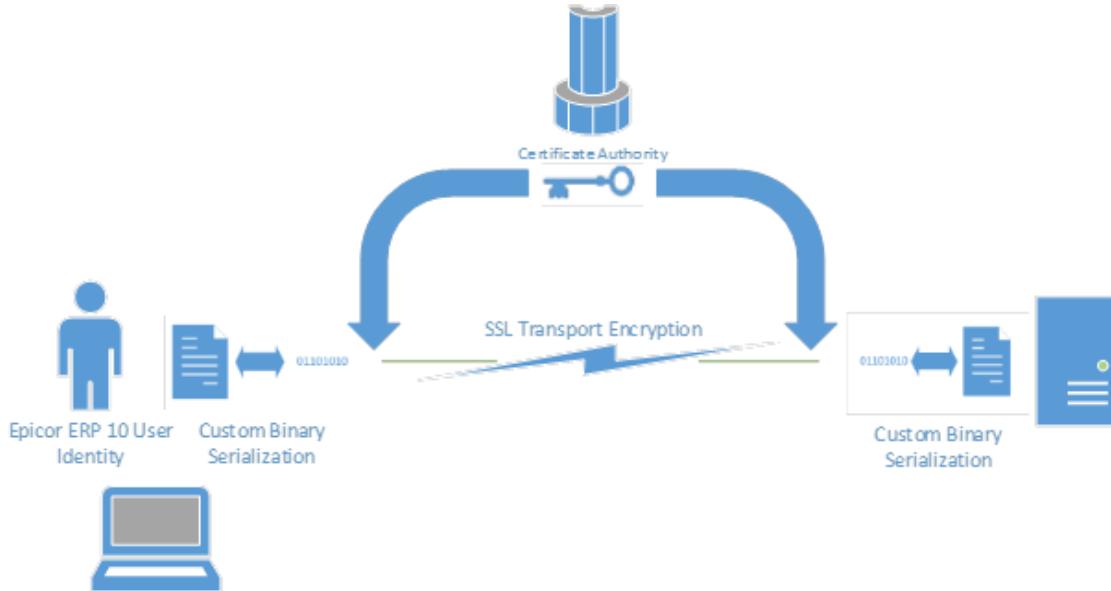
Protocol binding features:

- Client Windows Domain credentials are required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The serialized data is compressed through a custom routine developed by Epicor.
- Windows encrypts the transport between the client and the server.

## UsernameSSLChannel

This NET.TCP binding authenticates transactions using a Secure Sockets Layer (SSL) X509 certificate. Leverage this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor application.

The following diagram illustrates how this binding handles network transactions.



### Protocol binding features:

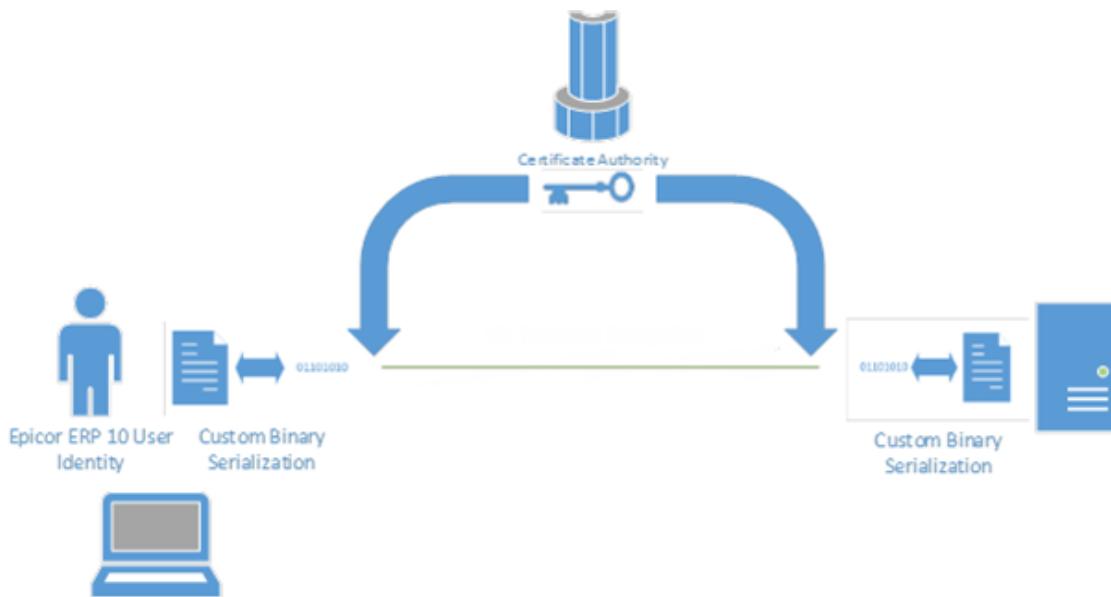
- Epicor user account (User ID/Password) token required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The Secure Socket Layer encrypts the transport between the client and the server.

## HttpBinaryUsernameSslChannel

This HTTP binding protocol authenticates using a Secure Sockets Layer (SSL) X509 certificate. The data transfers between the client and server using Hypertext Transfer Protocol (HTTP). Instead of the transport, the message which contains the data transfer is encrypted. Because this binding does not use Hypertext Transfer Protocol Secure (HTTPS), it tends to be slower than bindings which use HTTPS.

Use this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor ERP application.

The following diagram illustrates how this binding handles network transactions.



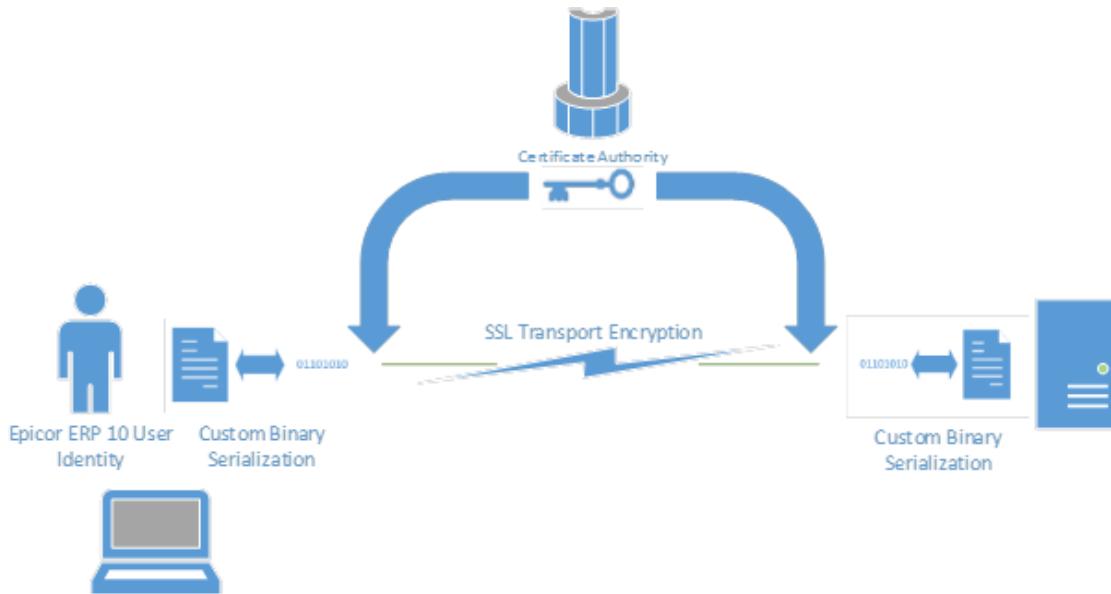
Protocol binding features:

- An HTTP based protocol.
- Epicor user account (User ID/Password) token required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The protocol uses .NET v4.5 compression.
- The message body is encrypted; message headers are not encrypted; the transport is not encrypted.

## HttpsBinaryUsernameChannel

This HTTPS binding authenticates transactions using an Epicor Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). HTTPS encrypts the data transfer.

The following diagram illustrates how this binding handles network transactions.



Protocol binding features:

- Epicor user account (User ID/Password) token required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The protocol uses .NET v4.5 compression.
- HTTPS encrypts the transport between the client and the server.

## HttpsBinaryWindowsChannel

This HTTPS binding authenticates transactions using a Windows Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

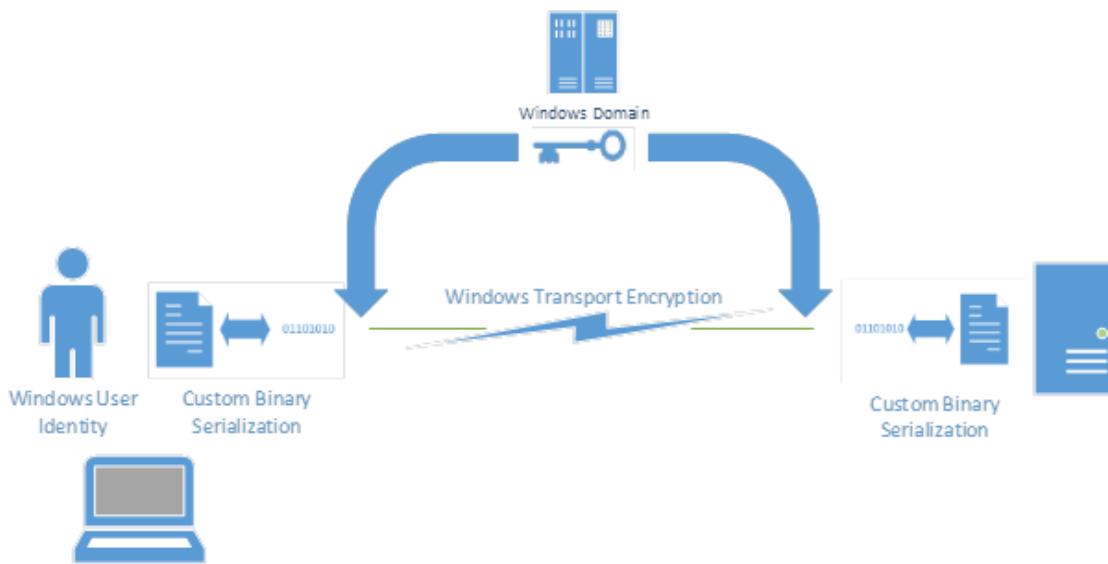
You can select this method for application servers that handle smart client installations and Epicor Web Access (EWA) installations where users access the application through the same domain. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.

You set up this protocol using a **Domain User Account**. This account can be either a custom account contained within an application pool (AppPool) or a built-in account that runs through the **LocalSystem**, **LocalService**, or **NetworkService**. Built-in accounts automatically contain security verification to work within their selected local or network service. Custom accounts typically have more powerful security, but they can require more manual set up as well.

If you use a custom account with **Kerberos** authentication, this Domain User Account must also have a **Service Principal Name** (SPN) to complete the security verification. While built-in accounts automatically receive an SPN when created, you often must manually generate SPNs for custom accounts. You do this by running the **setspn.exe** utility. Setspn is a command-line tool you activate through the Command Prompt or PowerShell windows.

 **Tip** When you do not have an SPN value for your Domain User Account, you receive an SSPI context error. Review the Microsoft documentation available on the internet for details on how to resolve this error.

The following diagram illustrates how this binding handles network transactions.



### Protocol binding features:

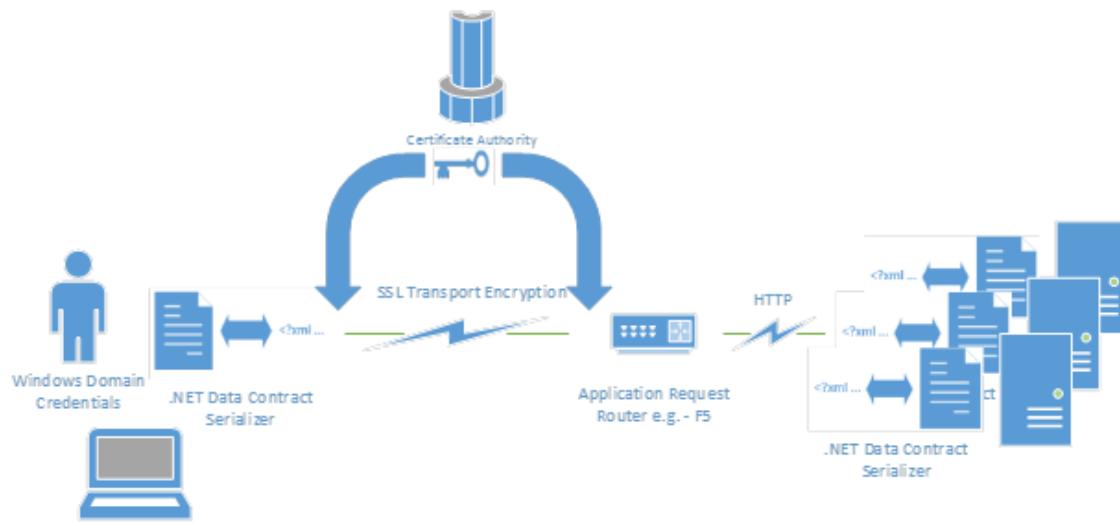
- Client Windows Domain credentials required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The protocol uses .NET v4.5 compression.
- Windows encrypts the transport between the client and server.
- The client-server communications is based on HTTP.

## HttpsOffloadBinaryUserNameChannel

This HTTPS protocol binding is a configuration that offloads encryption handling to an intermediary Application Request Router such as an F5.

The binding authenticates using an Epicor Username and Password token. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

The following diagram illustrates how this binding handles network transactions.



Protocol binding features:

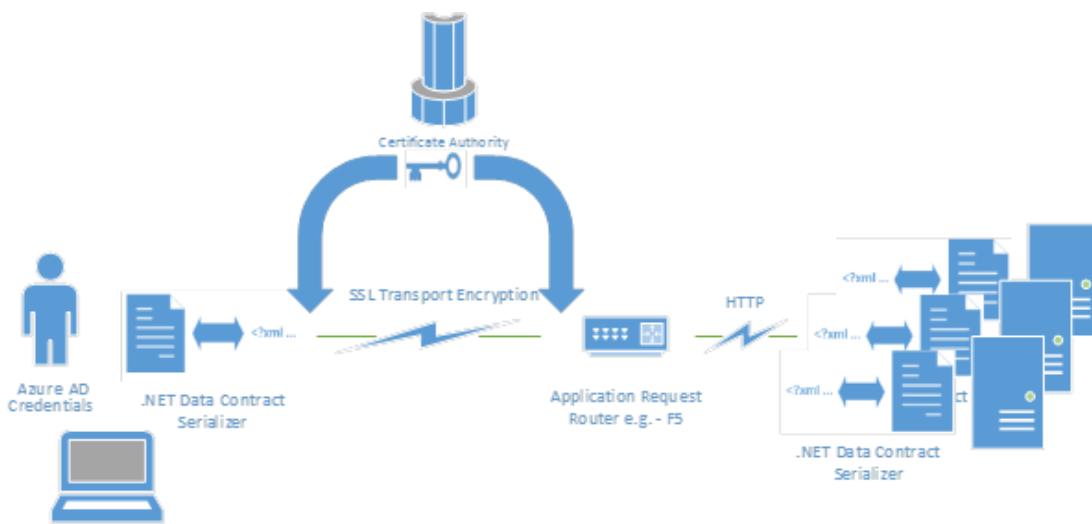
- Epicor user account (User ID/Password) token required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The transport is encrypted between the client and Application Request Router (or F5) Server.
- The data traffic between the ARR server and the Epicor application server is not encrypted.

## HttpsOffloadBinaryAzureChannel

This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an intermediary Application Request Router such as an F5.

The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Azure AD. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

The following diagram illustrates how this binding handles network transactions:



#### Protocol binding features:

- Azure AD security token required for authentication.
- The protocol is an Epicor Custom Binary Serialization.
- The transport is encrypted between the client and Application Request Router (or F5) Server.
- The data traffic between the ARR server and the Epicor application server is not encrypted.



**Important** When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the **AddressFilterModeAny** node in web.config as shown below:

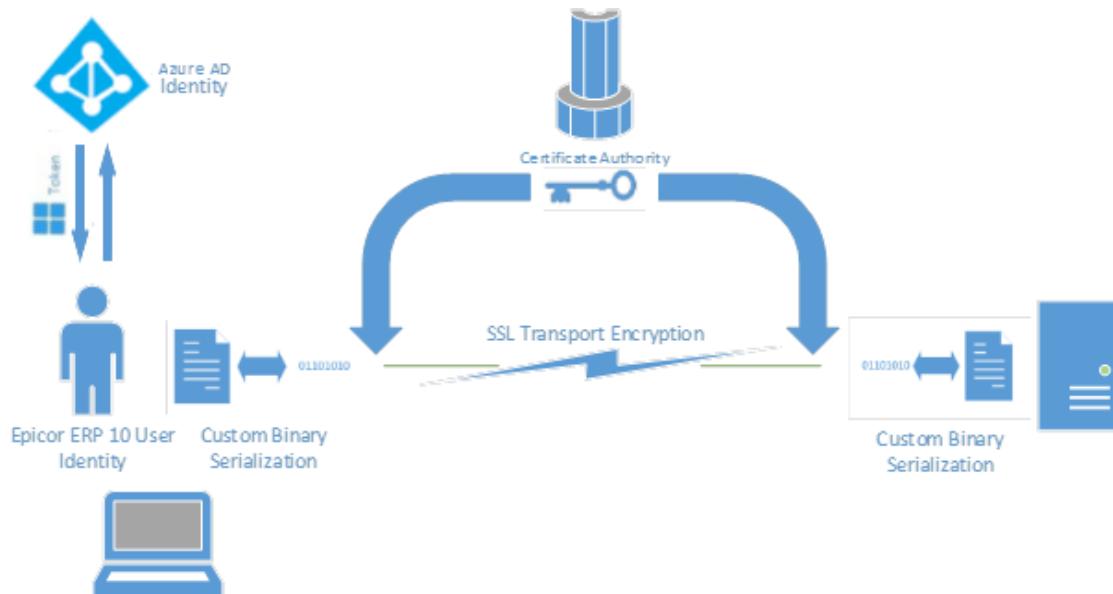
```
Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens
<AddressFilterModeAny />
```

#### HttpsBinaryAzureChannel

Use this protocol to enable authentication of ERP application users against users in Microsoft Azure Active Directory (Azure AD).

This binding relies upon the user authenticating against Azure Active Directory and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

The following diagram illustrates how this binding handles network transactions:



#### Protocol binding features:

- HTTPS encrypts the transport between the client and the server.
- The protocol uses .NET v4.5 compression.
- Security token lifespan is controlled by Azure AD.

## SSL Certificates with Multiple Sites

If you use .NET 4.6.1 or later with either the **UsernameSslChannel** or **HttpBinaryUsernameSslChannel** bindings, you can create certificates that contain additional host names.

The .NET system checks the SSL certificate for these additional host names detailed in a **Subject Alternative Names** (SAN) field. You typically create a SSL certificate in this way to secure multiple sites across different domains. However due to conflicts with systems that use older SSL certificates, this feature is disabled in Epicor ERP.

To use this .NET 4.6.1 feature, activate this **<appSettings>** option in the client .syconfig file:

- **<EnableMultipleDnsEntriesInSancertificate value="True"/>**

The client installation can now use the multiple sites defined in the SAN field for the SSL certificate. The system checks the **Domain Name System** (DNS) identities for each site included in the certificate, establishing a connection with these sites.

## Custom Bindings

The Epicor application supports custom bindings on client installations. This custom binding is a class you define in the Epicor.ServiceModel. Each service has this class so that the server installation can use the custom binding to connect with the client installation.

### Server Binding

To set up a custom binding, you first modify the **web.config** file on the server installation so it identifies both the custom binding and your binding configuration.

The web.config file is found on your server machine in the **C:\Epicor\[YourEpicorVersion]\Server** directory path. Enter the following template, and substitute the **[ServerBindingName]** with the name of your custom binding configuration:

```
<system.serviceModel>
    <protocolMapping>
        <remove scheme="https" />
        <add scheme="https" binding="customBinding" bindingConfiguration=
"[ServerBindingName]" />
    </protocolMapping>
```

This binding configuration must exist in the <bindings>/ <customBinding> node. This node is also found within the web.config file.

```
<binding name="[ServerBindingName]" openTimeout="00:10:00" receiveTimeout="9:00
:00" sendTimeout="9:00:00">
    [Details for the binding definition]
</binding>
```

The following example illustrates a custom binding configuration:

```
<binding name="ServerBindingName" openTimeout="00:10:00" receiveTimeout="9:00:0
0" sendTimeout="9:00:00">
    <binaryMessageEncoding compressionFormat="Deflate">
        <readerQuotas maxDepth="50" maxArrayLength="2147483647" maxBytesPerRe
ad="2147483647" />
        </binaryMessageEncoding><security authenticationMode="UserNameOv
erTransport" />
        <httpsTransport maxReceivedMessageSize="2147483647" maxBufferSize="21
47483647" />
    </binding>
```

### Client Binding

You next modify the **.sysconfig** file for the client installation.

This file is found on the client machine in the **C:\Epicor\[YourEpicorVersion]\Client\Config** folder. Enter the following template in the .sysconfig file. Substitute the **[ClientBindingName]** value with the name of your custom binding:

```
<system.serviceModel>
    <bindings>
        <customBinding>
            <binding name="[ClientBindingName]">
                [Details for the binding definition]
            </binding>
        </customBinding>
```

```
</bindings>
</system.serviceModel>
```

Once you have entered this custom binding, enter the custom name in the endpoint binding setting:

- <EndpointBinding=" [ClientBindingName ] ">

For example, if you create the ClientBindingName protocol, you enter code similar to the following:

```
<system.serviceModel>
  <bindings>
    <customBinding>
      <binding name="ClientBindingName">
        <binaryMessageEncoding compressionFormat="Deflate">
          <readerQuotas maxDepth="50" maxArrayLength="2147483647"
" maxBytesPerRead="2147483647" />
          </binaryMessageEncoding>
          <security authenticationMode="UserNameOverTransport" />
          <windowsStreamSecurity />
          <tcpTransport maxReceivedMessageSize="2147483647" maxBufferSize="2147483647" transferMode="Buffered" />
        </binding>
      </customBinding>
    </bindings>
  </system.serviceModel>
```

# System Tasks

---

This section of the System Administration Guide describes specific tasks you need to run on your SQL Server machine. It begins by documenting how you set up additional application servers and then describes how you back up your databases.

## Server Security

---

Microsoft SQL Server is the system you use to manage the databases for the Epicor ERP application. You need to manage user permissions and access to SQL Server to ensure this core system maintains its data integrity.

Most users do not need security access to the database, as the Epicor ERP application, including its reports and processes, can be run by all users. End users access the application through a single SQL Server login defined in the connection string for a specific application server; each login account is set up internally through User Account Security Maintenance. Only grant permissions to users who will help manage the Epicor databases.

This section of the guide explores assigning SQL Server security access to database managers. Use these features to determine which users can access the SQL Server databases, and the level of permissions for each administrator account. You can give users varying degrees of access to both SQL Server and each database.



**Tip** For information on how to administer security on SQL Server, review the **SQL Server 2012 Security Best Practices - Operational and Administrative Tasks** white paper. This white paper is available for download from Microsoft. It details the security strategies you can implement. It is also recommended you review the **SQL Books Online** information to become familiar with the SQL Server administration functionality.

## Prerequisites

The following instructions describe how to create administration accounts for SQL Server. They assume you have installed the Epicor ERP application and have created a database for the application.

If you have not yet set up these items, follow the steps documented in the Epicor ERP Installation Guide. This guide is available to download from EPICWeb. You will need to enter your EPICWeb user account and password:

- <https://epicweb.epicor.com/products/epicor-erp/downloads>

## Administration Account

The primary SQL Server account you create is the Administration Account. This key account has access to the tools and features you need to manage SQL Server for your organization.

The following example illustrates how you set up a SQL Server administrator account that has a database creator role.

### Create Account

You create login accounts through Microsoft® SQL Server Management Studio®.

1. Launch **Microsoft SQL Server Management Studio**.  
The **Connect to Server** window displays.

2. Click the **Server** name drop-down list and select the server you need to manage.
  3. Now click the **Authentication** drop-down list to indicate how you will logon to SQL Server.
    - **Windows Authentication** – Select this option to login using your Windows account. Your Windows account displays by default and you cannot change these values.
    - **SQL Server Authentication** – Select this option to login using an administrator account you set up for SQL Server. Once you select this option, you need to enter your **Login** and **Password**.
  4. Click the **Connect** button.  
The **Object Explorer** tree view pane displays management items for the selected database.
  5. Expand the **Security** node and the **Logins** node.  
A list of the current login accounts displays.
  6. Right-click the **Logins** node; from the context menu, select the **New Login...** option.  
The **Login - New** window displays.
  7. Enter the **Login** name for the account; enter EpicorAdmin.
  8. Now indicate whether this account will use **Windows authentication** or **SQL Server authentication**.
    - If you select Windows authentication, this user logs in using a default Windows account.
    - If you select SQL Server authentication, enter the **Password** this new account will use. Enter a Password that's at least eight characters long and then enter this value again in the **Confirm password** field.
  9. By default the **Enforce password policy** check box is selected. This indicates a number of password rules are active, including that the password must be at least eight characters long and it must contain upper case, lower case, and numeric characters.
-  **Tip** For complete details about password complexity, review the **Password Policy** topic in SQL Server books.
10. Clear the **User must change password at next login** check box. The user can now enter the same password you created for the account.

The new login account is created. You next define the server roles for this account.

## Assign Server Roles

Server roles define the SQL Server permissions granted this new login account. Microsoft SQL Server installs with a series of fixed server-level roles you can assign to each account.

Server roles are maintained by database administrators. They function like groups. Each role has a permission level that defines how much administrative control role members have in SQL Server. These permissions apply to the entire server, and not to an individual database file.

To assign server roles:

1. Within the **Login - New** window, on the **Select a page** tree view pane, click the **Server Roles** node.  
The server roles display.
2. Select the server roles you wish to assign to this login account.

Available fixed server-level roles and their permissions:

- **BulkAdmin** - Can run the BULK INSERT statement. By leveraging this statement, users can import a data file into a database table or database through a user-specified format.
- **DBCreator** - Can create, modify, drop, and restore databases.
- **DiskAdmin** - Manages SQL Server disk files.
- **ProcessAdmin** - Can end active processes on the server.
- **Public** - The default server role; all login accounts are automatically members of this role. This setting cannot be changed; you can only add additional server roles to the login account.
- **SecurityAdmin** - Manages login accounts and their properties. These users can reset passwords and grant, deny, and revoke server permissions. If they have access to a database, these users can also grant, deny, and revoke database permissions.
- **ServerAdmin** - Modifies server configuration settings and can shut down SQL Server.
- **SetupAdmin** - Can add or remove linked servers. Can also manage SQL Server startup options and tasks.
- **SysAdmin** - Performs any administrative task on SQL Server.

3. Because this account will manage SQL Server, select the **DBCreator** option.

## Assign User Mappings

To further define security settings, you define what databases each login account can access.

Besides mapping the login account to specific databases, you can also assign database roles. Like server roles, database roles define user permissions. However these permissions define the user's access for the selected database. Each user can have a different database role for each database.

To map databases and assign database roles:

1. Within the **Login - New** window, on the **Select a page** tree view pane, click the **User Mappings** node. The databases currently available on the system display.
2. From the **Users mapped to this login** list, select the databases this login account can access. To do this, select the **Map** check box next to each database for which you want to grant access.
3. Now assign the database roles you wish to assign to this login account. Each database role defines a set of permissions this user has on the database.

Available database roles:

- **db\_accessadmin** - Can add or remove database access for Windows logins, Windows groups, and SQL Server logins.
- **db\_backupoperator** - Can create and manage database backups.
- **db\_datareader** - Can read the data from user tables.
- **db\_datawriter** - Can add, delete, or modify the data in the database user tables. Most users should not have these rights, as they will not need to write to the Epicor database. Only assign these rights to user accounts used for the application pool.
- **db\_ddladmin** - Can run Dynamic-Link Library (DDL) commands in the database.
- **db\_denydatareader** - Prevented from reading the data in the database user tables.
- **db\_denydatawriter** - Prevented from adding, deleting, or modifying the data in the database user tables.
- **db\_owner** - Can perform configuration and maintenance on the database.

- **db\_securityadmin** - Can modify database roles and manage permissions for the database.
- **public** - The default database role; all login accounts are automatically members of this database role. This setting cannot be changed; you can only add additional database roles to the login account.

4. Because this account will manage SQL Server, select the **db\_securityadmin** option.
5. When you finish, click **OK**.

## Database Manager Account

You may also want to create a Database Manager account. Users who log in with this account have limited access to SQL Server, but they can still administrate selected databases.

This account will have the default Public server role, but then have a number of database roles.

### Create Account

The following steps illustrate how you create a database manager account.

1. Right-click the **Logins** node; from the context menu, select the **New Login...** option.  
The **Login - New** window displays.
2. Enter the **Login** name for the account; enter EpicorRuntime.
3. Select **SQL Server authentication** and enter the **Password** for this new account. As described previously, enter a Password that's at least eight characters long.
4. Enter this value again in the **Confirm password** field.
5. Click on the **Server Roles** node.  
The server roles display.
6. This account will not be used for SQL Server administration, so just verify the default **Public** role is selected.
7. Now on the **Select a page** tree view pane, click the **User Mappings** node.  
The databases currently available on the system display.
8. From the **Users mapped to this login** list, select the databases this login account can access. To do this, select the **Map** check box next to each database for which you want to grant access.
9. Now assign the database roles you wish to assign to this login account.  
Because this account will be used for database management, select these database roles:
  - **db\_datareader** - Can read the data from all user tables.
  - **db\_datawriter** - Can add, delete, or modify the data in the database user tables.
  - **db\_ddladmin** - Can run Data Definition language (DDL) commands in the database.
  - **public** - The default database role; all login accounts are automatically members of this database role. This setting cannot be changed; you can only add additional database roles to the login account.
10. When you finish, click **OK**.

Besides these login accounts, you typically would create other accounts for users who handle database backups, data replication managers, and other roles. Consider the needs of your organization and create the SQL Server accounts you require to manage the entire system.

## Create an Application Server

---

An application server manages how a specific instance of the Epicor ERP application runs. Through each application server, you can configure licenses, companies, sessions, and users for a specific database.

The Application Server Setup window contains the settings you use to add a new application server, update an existing application server, or review the current application server's properties. You also use this program to configure any extensions for use with the current application server -- such as Epicor Web Access, Epicor Data Discovery, or Epicor Education. The following Add Extensions section details how you add these items to an application server.

You can set up multiple application servers to run the same database and balance the load. For example, you create two application servers for the same database, but these application servers are linked to different server machines through their endpoint bindings. One application server is set up to run Epicor Web Access (EWA) on one server machine, while another application server is set up to run a smart client through Net.TCP on a different server machine. Likewise you could set up another application server that links to a machine which only handles SSRS reporting tasks.

### Prerequisites

The following instructions describe how to add a new or existing application server to your system. They assume you have installed the Epicor ERP application and have already installed at least one application server.

Note to add or update an application server, these items must be installed on your system:

- **Epicor ERP Database** - At least one database must be mounted on the database server for the Epicor ERP application. Your new or existing application server will connect to this database. You set up databases within the **Epicor Administration Console**.
- **System Agent** - A system agent must be running inside the Epicor ERP application. This system agent connects the application to the database. You set up the system agent within the application by launching **System Agent Maintenance**.

If you have not yet set up these items, follow the steps documented in the Epicor ERP Installation Guide. This guide is available to download from EPICWeb. You will need to enter your EPICWeb user account and password:

- <https://epicweb.epicor.com/products/epicor-erp/downloads>

### Add Servers

To begin, an Epicor Server must be available. You can then add one or more application servers to the Epicor Server.

The following instructions describe how to add an Epicor Server to your system. If your system already has the Epicor Server you need, skip to step 8 below to launch the **Application Server - Create Site** window.

1. Log into your Epicor ERP application server.
2. Launch the **Epicor Administration Console**.
3. Now from the tree view on the left side, select the **Server Management** node.

4. Right-click this node to display the context menu; select **Add Epicor Server**. The **Add Epicor Server** window displays.
5. By default, the server **Name** displays its full qualified domain name. Do not change this value.
6. The **SSL Cert** field contains the name of the SSL Certificate that is assigned to the **https** binding (if available) of the web site under which the ERP application server is hosted in IIS Manager. If no certificate is selected or if you want to use another certificate, click the **Browse (...)** button. In the SSL Certificate Options dialog, either click **Pick an existing SSL Certificate** or **Generate a new Self Signed Certificate** depending on your requirements.
  - **Pick an existing SSL Certificate**- the Select a Certificate dialog displays the available certificates. Select the certificate you want to use for Epicor Server and click **OK**.



**Important** The SSL certificate you pick must have a Friendly Name assigned so that the Epicor ERP server could recognize it. For information on how to verify and assign a Friendly Name to a certificate, review the Troubleshooting section in the System Administration Guide or the Epicor ERP 10.1 Installation Guide.

- **Generate a new Self Signed Certificate** - enter a name to identify your certificate and the number of years it will remain valid, and then click **Create Certificate**.

When you select or generate a self signed certificate, the system adds the https binding type to the web site under which the ERP application server is hosted and assigns it with this certificate.



**Note** If you want to review the available Site Binding types, in IIS Manager, navigate to the web site under which the ERP application server is hosted (commonly this is the Default Web Site) and click **Bindings** in the **Actions Panel**. For more information on how to work with site bindings, refer to IIS Manager Help.

7. Click the **Ping Server** button to verify the server name.
8. A message displays that the connection is successful. Click **OK**.
9. Now from the tree view, right-click your Epicor server; from the context menu, select **Add Application Server**.

The **Application Server - Create Site** program displays. You use this program to define the values you will use on the application server. The next topics explain what you set up on each tab on this window.



**Important** If another user is updating the same application server, a Setup dialog box displays while it launches that indicates the setup data is currently being modified by this user. Click **No** to exit the Application Server Setup window. If you click **Yes** and launch this program, only the most recent changes are saved to the application server settings. Because of this, you may lose your changes.

## Application Server Settings

Use the fields on the Application Server Settings sheet to define the main options for the current application server.

You can modify the following settings:

1. You first enter or select the **Application Name**. This value is the name Internet Information Services (IIS) uses to create the application, and this value is also added to the URL address which the client installation uses to connect to the local or remote application server. For example, if you enter Epicor10 in this field, the application server URL will be net.tcp://<servername>/Epicor10.

Notice you can directly enter the name or click the **Browse** (...) button to find and select it.

When you change the value in this field, both the **Web Site Directory** and the **Application Pool Name** fields update with this name change as well. This feature prevents a site that already exists from being overwritten by the name change.

2. Enter the **Deployment Directory** that contains the Epicor server installation. For example:  
**\EpicorServer\Epicor\Epicor10.2.200.**



**Important** Be sure you are a member of the **Administrators** group on the server you enter in this field.

3. Use the **Deployment Version** drop-down list to select your update version from the list of updates available on your server. It is recommended that you select the latest update. If no updates are available, select the **Base** option.

Note that when you click **Deploy**, the application server updates the Epicor ERP application to the selected version. If prompted that all users will be disconnected while the system updates, verify all users have logged out of the system and then click **Yes** to continue. Some settings will also return to their default values; for example, the Locktimeout value in the web.config file will return to its default 180000 value.

4. Now define the **Web Site Directory** on the server machine that contains the application server. The application server is installed in this location. For example: **C:\Inetpub\wwwroot\Epicor10.**



**Important** If you are creating or updating an application server and a Web Site Directory already exists, a message displays asking if you wish to overwrite it. Click **Yes** to overwrite the existing site with the new web site location. Click **No** to keep the original site.

5. Define how this application server checks for authentication certificates through Internet Information Services (IIS) by selecting an option from the **Endpoint Binding** drop-down lists. When a user logs into the application, the selected protocol option checks whether the user can access the Epicor application.

Epicor offers three types of protocols: Net.Tcp, Http, andHttps. You can select one protocol binding option for each type. You then select the binding for deploying Admin Console on the Admin Console Settings sheet. To deploy extensions, the system uses the first selected type. For example, if you select an Http and anHttps protocol option and leave the Net.Tcp field blank, the system will use the Http option you selected. Other selected options can be used later to connect client installations to your application server.



**Tip** For more information on how you set up each binding option, review either the **Epicor 10 Architecture Guide** or the **System Administration Guide**.

Available options:

- **Net.Tcp Endpoint Binding:**
  - **UsernameWindowsChannel** - This NET.TCP binding authenticates transactions through an Epicor Username and Password. Windows checks for existing Epicor user accounts to authenticate logins.
  - **UsernameSSLChannel** - This NET.TCP binding authenticates transactions using a Secure Sockets Layer (SSL) X509 certificate. Leverage this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor application.

Selecting this option causes the **SSL Certificate Subject Name** and **DNS Endpoint Identity** fields to appear. You use these fields to enter the name of your SSL certificate and the identity of the server.

- **Windows** - This NET.TCP binding authenticates transactions using a Windows Username and Password. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.

- **Http Endpoint Binding:**

- **HttpBinaryUsernameSslChannel** - This HTTP binding protocol authenticates using a Secure Sockets Layer (SSL) X509 certificate. The data transfers between the client and server using Hypertext Transfer Protocol (HTTP). Instead of the transport, the message which contains the data transfer is encrypted. Because this binding does not use Hypertext Transfer Protocol Secure (HTTPS), it tends to be slower than bindings which use HTTPS.

Use this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor ERP application.

Selecting this option causes the **SSL Certificate Subject Name** and **DNS Endpoint** Identity fields to appear. You use these fields to enter the name of your SSL certificate and the identity of the server.

- **HttpOffloadbinaryUserNameChannel** - This HTTP protocol binding is a configuration that offloads encryption handling to an intermediary Application Request Router such as an F5.

The binding authenticates using an Epicor Username and Password token. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

- **HttpsOffloadBinaryAzureChannel** - This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an intermediary Application Request Router such as an F5.

The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Azure AD. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

 **Important** When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the **AddressFilterModeAny** node in web.config as shown below:

```
Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens
<AddressFilterModeAny />
```

- **HttpsOffloadBinaryIdpChannel** - This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an intermediary Application Request Router such as an F5.

 **Important Epicor Identity Provider** is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available **internally** to Epicor.

The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Epicor Identity Provider deployment. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

 **Important** When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the **AddressFilterModeAny** node in web.config as shown below:

```
Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens
<AddressFilterModeAny />
```

- **Https Endpoint Binding:**

- **HttpsBinaryUsernameChannel** - This HTTPS binding authenticates transactions using an Epicor Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). HTTPS encrypts the data transfer.

- **HttpsBinaryWindowsChannel** - This HTTPS binding authenticates transactions using a Windows Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

You can select this method for application servers that handle smart client installations and Epicor Web Access (EWA) installations where users access the application through the same domain. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.

- **HttpsBinaryAzureChannel** - Use this protocol to enable authentication of ERP application users against users in Microsoft Azure Active Directory (Azure AD).

This binding relies upon the user authenticating against Azure Active Directory and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

- **HttpsBinaryIdpChannel** - Use this protocol to enable authentication of ERP application against Epicor Identity Provider (IdP).



**Important Epicor Identity Provider** is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available **internally** to Epicor.

This binding relies upon the user authenticating against IdP and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

6. When you select the **UsernameSslChannel** for the **Endpoint Binding**, the **SSL Certificate Subject Name** field displays. Use this field to enter the Subject Name of your Secure Sockets Layer (SSL) certificate; you can directly enter this name or click the **Browse (...)** button to find and select it.

After you finish setting up the application server and click **Deploy**, the server's web.config file updates with this Subject Name. This value displays under the <behaviors> node in the <serviceCertificate> setting.

7. Likewise when you select the **UsernameSslChannel** for the **Endpoint Binding**, the **DNS Endpoint Identity** field also displays. This field specifies the expected Domain Name System (DNS) identity of the server. When an application server uses a Secure Sockets Layer (SSL) Certificate for endpoint binding, you must enter this identity value.

When the system runs X509 SSL Certificate authentication, it uses this identity value to validate the application server. If the SSL certificate contains a DNS Endpoint Identity with the same value, the application server is valid and can be accessed by its task agent.

8. If you have custom programs to incorporate with the Epicor ERP application, enter the **Custom Directory** that contains these custom .dll files. You can enter this path directly or click the **Browse (...)** button to find and select this path.

You can also enter a relative path in this field. This base path is the directory from where the application server runs. Through the **web.config** file, you can define custom directories that then populate this field as well. For details on how to enter this relative path or use the web.config file, review the **Custom Directory** definition in the following **Fields** topic.

After you click **Deploy** on this window, these custom .dll files are included in the Epicor ERP application.



**Tip** As a best practice, you should always place custom programs in this separate Custom Directory. Then the next time the application version is updated, these custom programs are not overwritten. You can then modify these custom programs to work with the new version.

**9.** Select the **Shared Assembly Location** check box if you have a network load balanced environment.

For example, you may have the Epicor ERP application installed on multiple servers. You then must have a central directory that contains all the server assemblies and Business Process Management (BPM) folders. If your server environment is set up this way, activate this check box.

You typically select this check box when you add your second and subsequent application servers. When you install the first application server, the install process creates a **Server/Assemblies** folder. You then create a Windows share for this folder. When you add more application servers, you select this check box and then enter or select this shared assembly folder location.



**Tip** You can move the Assemblies folder to some other disk location. However if you move this folder, you must manually update the web.config file for the first application server so it points to this new location.

**10.** If you select the Shared Assembly Location check box, you also activate the **Shared Directory** field. Use this field to define the directory which contains the server assemblies and BPM folders. You can enter this path directory or click the **Browse** (...) button to find and select it.

**11.** The **Application Pool Name** is the name of the application pool associated with the new or updated application server.

It defines a group of related URLs that use the same process or set of processes. The new application server must be placed in an application pool.

By default, this field uses the value you entered in the **Application Name** field. To change this value, click the **Browse** (...) button next to it. In the **Select Application Pool** dialog window, select the application pool you wish your application server to be associated with from the list of available pools.



**Note** The **Application Pool** drop-down list displays all application pools that satisfy your application server requirements. For example, you will only see the pools with matching .NET CLR version in the list. The properties of the selected application pool can be viewed in the **Properties** field of this dialog window.



**Tip** Use this functionality if you need to share one application pool across two or more application servers.

**12.** If you need to enter a specific user account for the Internet Information Services (IIS) application pool this application server uses, select the **Use Custom Account** check box. Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.

If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the **LocalSystem** account. If you do not use an SSRS server, the connection uses the **ApplicationPoolIdentity** account.

**13.** The **Current Deployment** section details the state of the application server. Review the information in these fields:

- a. **Status Indicator** - This icon indicates whether the application server is **Not Installed** (red) or **Installed** (Green).

- b. **Installed On** - Displays the date on which the application server was installed.
- c. **Server** - Contains the name of the server on which the application server is installed.
- d. **Version** - Displays the version number for the application server. Use this value to compare against the current application server available from Epicor; if you have an older version, consider updating the application server.

**14.** You next set up the **Database Connection** for this application server. Click this tab.

## Database Connection

You use the settings on the Database Connection sheet to define how the current application server interacts with the database.

You can modify the following settings:

1. Select the **Server Name** for the database SQL server instance that contains the SQL database you will use with the new application server.
2. Now click the **Authentication** drop-down list and select either the Windows Authentication or SQL Server Authentication option.
  - a. If you select **Windows Authentication**, the **User** and **Password** default to the account used for the application pool, and these fields are disabled.
  - b. If you select **SQL Server Authentication**, enter the **User** and **Password** you use to log into SQL Server.
3. Now from the **Database Name** drop-down list, select the name of the SQL database you will link to this application server. All the databases available under the selected SQL Server instance display on this drop-down list.
4. To verify the application server can connect with this database, click **Test Connection** and click **OK** in the confirmation message.
5. A dialog box displays indicating the test was successful. Click **OK**.
6. You next set up the **Admin Console Settings** for this application server. Click this tab.

## Admin Console Settings

You use the Admin Console Settings sheet to modify the application server settings used by the Epicor Administration Console.

You can modify the following settings:

1. For the **Display Name**, provide a display name that will identify the application server in the administration console. Choose a name that helps you identify the purpose for the application server.
2. Enter the **Epicor User Name**. This value defines the user name for the Epicor user account that will access the application server.
3. Now enter the **Password** for the user account used to access the application server. The password is stored in an encrypted format.

4. From the **Endpoint Binding** drop-down list, select a binding protocol to use for Admin Console. The available options include the endpoint bindings you selected on the Application Server Settings sheet.
5. Enter the **Operation timeout** value you want for the application server. This value determines the wait time until an incomplete operation is aborted by the application server. The default value is 300 seconds.  
Get the correct value from the `<appSettings><OperationTimeOut>` element of the `.sysconfig` file that points to the application server. In your Epicor application installation, `.sysconfig` files are located in the `client\config` folder.
6. Select or clear the **Validate WCF Certificate** checkbox to match the value set in the `<appSettings><WCFCertValidation>` element of the `.sysconfig` file:
  - **Select** the checkbox if `<WCFCertValidation value="True" />`.
  - **Clear** the checkbox if `<WCFCertValidation value="False" />`.
7. For **DNS Identity** value, enter the expected DNS server name. Scenarios where you need to enter a value in this field:
  - **UsernameSSLChannel Selected in Endpoint Binding** - When authenticating using message-level or transport-level Secure Sockets Layer (SSL) with X.509 certificates, WCF ensures that the certificate provided during the SSL handshake contains a DNS or Common Name (CN) attribute equal to the value specified in this field.
  - **Windows Selected in Endpoint Binding** - When the service authenticates using message-level or transport-level SSL with a Windows credential for authentication, and negotiates the credential, then the negotiation passes the service principal name (SPN) so that the DNS name can be checked. The SPN is in the form host/<dns name>.  
Get the correct DNS server name from the `<appSettings><DnsIdentity>` element of the `.sysconfig` file.
8. Optionally in the **Epicor Application Launcher** section, indicate how you will connect the **Epicor Administration Console** to the Epicor application. If you activate this feature, you can launch **User Account Security Maintenance** from within the console. When you expand the **Users** node, select a user, and then select **Properties** from either the context menu or the **Actions** pane, User Account Security Maintenance displays with the selected user account. Select one of the following options:
  - a. **Do not allow access to user details** - The default option, select this radio button when you do not want to activate this feature. The Epicor Administration Console then cannot launch User Account Security Maintenance.
  - b. **Use Epicor Smart Client** - If you select this option, click the **Browse (...)** button to find and select the **Epicor.exe** file you will use to launch User Account Security Maintenance.
  - c. **Use Epicor Web Access** - If you use Epicor Web Access (EWA), select this option and click the drop-down list to define the URL for the web access. This drop-down list contains the web access values defined in the company configuration data for EWA (set within the client); you then launch the EWA version of User Account Security Maintenance.
9. You next set up the **Reporting Services** for this application server. Click this tab.

## Reporting Services

Epicor reports generate through SQL Server Reporting Services (SSRS). You set up the SSRS server options through the options on the **Reporting Services** tab.

You can modify the following settings:

1. Select the **Configure SSRS** check box to activate the SSRS fields. You can then define how this application server interacts with SSRS.



**Important** Be sure that once you select this check box, you continue to keep it selected during future updates to this application server. When any SSRS reports change as part of an update, these modified reports are automatically included when you deploy this update. If you clear this check box during a future update, it indicates you no longer use SSRS reporting, causing the application server to reconfigure without the SSRS functions.

2. Enter the **SSRS Web Service URL** for the SSRS Report Server. This value defines the Uniform Resource Locator (URL) for the server, so enter the web site location that contains it. When you install SQL Server, you set up this URL and so this value is typically **http://<localhost>/ReportServer**.

When you save, this URL location is validated. If the Application Server Setup program cannot find this location, an error message displays. Likewise if you clear the **Configure SSRS** check box, the setup program removes this URL location. If you activate the Configure SSRS check box again, you will need to restore this value.



**Tip** To find the value you need to enter in this field, go to the server machine and launch **Reporting Services Configuration Manager**. From the tree view, click the **Web Service URL** icon. The value you need displays in the Report Server Web Service URLs section. Copy this value into Notepad or a similar text editor so you can later paste it into the Application Server window. For example:  
`http://HVW12AS09:80/ReportServer`

3. Optionally, enter the **SSRS Reports Root Folder** location. This directory defines the root folder location where you will deploy the reports. For example, enter Epicor if you want the reports to deploy to the Epicor/Reports folder. If you leave the field blank, this root folder will be the directory that contains the report server home page file; the reports will deploy to the /Reports sub-folder in this directory.

4. Use the **Server Name** field to enter the name of the server where the SSRS database is located. The Epicor ERP application uses this database to generate SSRS reports.

5. Now click the **Authentication** drop-down list and select either the Windows Authentication or SQL Server Authentication option.

- a. If you select **Windows Authentication**, the **User** and **Password** default to your current login values.

To effectively connect with the server, this Windows user account must have access rights to the SQL Server. If this user account does not have access rights to the SQL Server, the report data cannot be generated and read from the report database.

- b. If you select **SQL Server Authentication**, enter the **User** and **Password** you use to log into SQL Server.

6. Use the **Report Database Name** to either enter or select the SQL Server database that will contain the temporary data used by SSRS to generate the report output. If the **Create DB** check box is selected, enter the database name in this field. If the Create DB check box is clear (not selected), click the **Down Arrow** next to this drop-down list; select the database you need from the list of options.

This database can be:

- **The same database used by the Epicor application** -- Although this set up is not recommended, your report server database can be the same as your main database.
- **A separate database on the SQL Server** -- This set up method is most common, as the report data then populates this separate database on the server.
- **A database on a different SQL Server** -- The report data from the Epicor application is sent to another server dedicated to SSRS report processing. If you are a larger organization, you may set up your system in this way to improve performance.



**Important** Do not select the system databases for the SSRS database, as these databases cannot store temporary report data. The system databases include:

- ReportServer
- ReportServerTempDB
- model
- msdb
- master
- tempdb

7. If you are setting up SSRS for the first time, select the **Create DB** check box. When you select this option and click **OK**, a new report database generates using the name you entered in the **Report Database Name** field. If you update the SSRS settings later on, you can select this database again or if needed, create a new database.

When you save, this database is validated. If the Application Server Setup program cannot find this database in the location you specified, an error message displays.

Note that when you register an existing application server, you cannot create a new report database. If you wish to create a new reports database for an existing application server, you must reconfigure it. To do this, right-click the application server and from the context menu, select **Application Server Configuration**. You can then enter a new Server Name and select the Create DB check box; after you click OK the new report database is generated.

8. When you finish defining your SSRS options, click the **Test Connection** button.

A message should display indicating that this application server is connected to SSRS. If you receive an error, check your values to make sure they are accurate and then test the connection again.

9. Verify the **Import Reports** check box is selected. This indicates you are ready to deploy your reports. These reports are placed in the server directory for the version. This server directory is a relative directory created where the software is installed. For example, if the install directory is D:\ERPSoftware\ERP10.2.200, then the reports install in this location: D:\ERPSoftware\ERP10.2.200\Server\reports.zip

This check box is clear (inactive) by default. You typically just select this check box when you first install SSRS on the current application server. After the first installation, you can then clear this check box. When you later install an update that includes changes to SSRS reports, these updated report definitions install in an update directory. For example: D:\Epicor\ERP10\ERP10.2.200\Updates\ERP10.2.200.1\Server\reports.zip

10. For the **SSRS ReportServer Location**, select the report server directory that contains the SSRS installation. If this directory path is on a remote machine, be sure this directory is shared; you can then both access and copy the report files to this folder.



**Important** You also need to have admin privileges on the report server machine to be able to start and stop reporting services when this is required by the system.

Depending on the SQL Server version you use, this location is similar to the following example directories. Notice they all use "ReportServer" for the folder name; substitute the folder name you use for the Epicor environment. Your specific directory path will be the name your system administrator assigned to the SQL Server instance during installation.

- **SQL Server 2017** -- C:\Program Files\Microsoft SQL Server Reporting Services\SSRS\ReportServer
- **SQL Server 2016** -- C:\Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\ReportServer
- **SQL Server 2014** -- C:\Program Files\Microsoft SQL Server\MSRS12.MSSQLSERVER\Reporting Services\ReportServer
- **SQL Server 2012** -- C:\Program Files\Microsoft SQL Server\MSRS11.MSSQLSERVER\Reporting Services\ReportServer
- **SQL Server 2008 R2** -- C:\Program Files\Microsoft SQL Server\MSRS10\_50.MSSQLSERVER\ReportingServices\ReportServer
- If the SSRS server is on a separate machine, enter the UNC path to the ReportServer directory. The current user account must have permissions to write to this remote directory. For example:  
\\<MachineName>\ReportServer

 **Important** If you have multiple SQL Server versions installed, make sure you select the location that matches the version used by the Epicor ERP application.

## Deploy the Server

When you finish entering or updating the application server settings on the Application Server Settings, Database Connection, Admin Console Settings, and Reporting Services sheets, you are ready to deploy the application server to the system.

### 1. Click Deploy.

The **Telemetry and License Data** message displays informing you that the telemetry tracking is enabled. To the message, click **OK**.

### 2. If you receive any errors, correct the set up information you entered and click **Deploy** again. When all errors are resolved, the program will finish the setup process.

If you receive any errors, correct the set up information you entered and click Deploy again. When all errors are resolved, the program will finish the setup process.

The following list contains possible errors and their solutions:

Error/Warning	Solution
Application Server Setup could not get a list of disk drive shares.	This occurs because the User Account Control (UAC) feature is active or the Windows Management Instrumentation service is not running. Either temporarily disable UAC or activate Windows Management Instrumentation. Now deploy the application server. When setup completes with no errors, be sure to activate UAC again.
Not enough disk space is available to install the application server.	Free up disk space on your server and then try deploying the application server again.
The system was not able to set up Token Authentication	This does not affect the deployment and the application server is installed correctly. To set up

The system was not able to deploy reports and configure SSRS. It offers you to restart the SSRS server.

Token Authentication manually, use the steps in the Configure Token Authentication topic.

This may happen when you choose a remote machine as an SSRS ReportServer Location. To fix this, agree to restart the SSRS server. Note that you must have admin privileges on the SSRS server machine.

**3.** This program now takes the values you entered to configure the application server.

Several values are written to the **web.config** file, and these values mainly define the connection string (`<connectionString>`) setting that links the application server to SQL Server. For example to ensure better performance, the SQL connection pool is set to a minimum pool size (Min Pool Size) of 100 threads and a maximum pool size (Max Pool Size) of 2,000 threads.



**Tip** If you need to review or update the web.config settings later, this file is located in the `...\\epicor\\<VersionNumber>\\Server` folder.

**4.** To finish registering your new application server, click the **Close** button.



**Important** Do not click either the **Cancel** button or the red "X" button. If you click these buttons, the Application Server Setup window exits without registering your new application server.

A status window displays the progress through the application server setup or update. In some situations, Internet Information Services (IIS) may need to stop and restart. This occurs because the setup process must update the **machine.config** file to use the default **machineSettings** timeout value (5 hours). To preserve the original settings, a **machine.config.backup** file generates first with your original settings. You can use this backup file to restore the original machine.config settings. These configuration files are located in the `C:\\Windows\\Microsoft.NET\\Framework\\<versionNumber>\\Config` folder.

When complete, a confirmation message appears stating you have registered the application server. If you are adding a new application server, a node is added to the tree view as the application server appears under the selected Epicor server.

The Epicor Administration Console next connects to the application server. When the connection is complete, the center pane displays the properties for the selected application server. The application server is installed/updated and active on your server.



**Tip** If the database uses a different version than the application server you are deploying, an error message generates in the **Windows Event Log**. This error message states the database and the application server are not synchronized; if the database uses an Epicor 9.xx version or earlier, the message also states the IceVer table cannot be found. To correct this error:

- If the message only states the database and the application server are not synchronized, install the latest Epicor ERP update and then deploy the application server again. Be sure the **Deployment Version** on the **Application Server Settings** sheet matches the current database version.
- If the message states the database and application server are not synchronized and the IceVer table cannot be found, first update the database using the **Database Migration** tool. This tool is located within the Epicor ERP directory in the **Utilities** folder. After you migrate the database to your current version, deploy the application server again.

## Add Extensions

---

You can extend your Epicor ERP environment through a series of add on installations. These installations include Web Access (EWA), Mobile Access, Enterprise Search, Epicor Education (Embedded Courses), Information Worker, Epicor Help, Data Discovery, and Web Configurator.

You configure these extended features through the Application Server Setup program. You add extensions through the child sheets under the **Extensions** tab.

### Install Extensions

After you have set up the application server, you can install Epicor ERP extensions. You install these extensions through the Epicor Administration Console.

1. Log into your server machine.
2. Launch the **Epicor Administration Console**.
3. Use the tree view to expand and select the **Server Management > [server] > [application server]** node.
4. Now from the **Actions** pane, click **Application Server Configuration**.
5. Click the **Extensions** tab.  
The **Web Access, Mobile Access, Enterprise Search, Epicor Education, Information Worker, Epicor Help, Data Discovery, and Web Configurator** tabs display.
6. Click the tab for the extension you wish to install. The following topics describe how you set up each extension.

### Web Access

Epicor Web Access™ displays programs as web forms within a browser window and is a significant part of the Epicor Everywhere Framework.

These forms are generated from Epicor ERP programs. Because of this, the appearance and functionality of the Epicor Web Access forms is nearly identical to the Epicor smart client programs, but do not require the installation of the Epicor client. Epicor Web Access programs can run on several operating systems and on a variety of devices - including handheld devices.

You can have multiple instances of the Epicor Web Access extension linked to each application server.

1. You use this sheet to install a new Web Access extension or add an existing extension. You can also update a Web Access extension so it connects properly with the current system.
  - a. To install a new extension, click the **New** button.  
The fields on the Web Access sheet activate for data entry.
  - b. To add an existing extension, click the **Browse (...)** button.  
The Application Server Settings program locates existing Web Access extensions; select the extension you wish to add. After you select the Web Access extension, the fields activate for data entry.
  - c. To update an existing extension, click the **Existing Deployment** drop-down list to select which Web Access extension you need to review or update.

2. If you need, enter the **Deployment Name** for this Web Access extension. Be sure to enter a name that helps you identify each Web Access extension available on this application server.
3. Now define the **Install Path** for this extension. Either enter this path or click the **Browse (...)** button to find and select the folder. The default install path is `\inetpub\wwwroot`.
4. Enter your site name in the **Web Site** field. If you do not have a name you wish to use, accept the Default Web Site value.
5. The **Virtual Directory** field displays the default name for the Epicor Web Access extension folder. You can change this value to any name that Internet Information Services (IIS) will accept. After you deploy the Web Access extension, a virtual directory is created in IIS using a physical path and the folder you define in this field. This physical path will be the **Install Path** directory.
6. By default the **Application Pool Name** uses the value you entered in the **Application Name** field on the **Application Server > Application Server Settings** sheet. You cannot change this value; it defines the name of the application pool associated with the application server that hosts this Web Access extension. An application pool defines a group of related URLs that use the same process or set of processes. The Web Access extension must be linked to an application pool.
7. If you need to enter a specific user account for the Internet Information Services (IIS) application pool this Web Access extension uses, select the **Use Custom Account** check box.  
Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter `MyDomain\UserName`. To connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you cannot stop and start the application pool.  
If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the LocalSystem account. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account.
8. If you will use Crystal Reports through this Web Access extension, select the **Enable Crystal Reporting** check box. You can then use both SQL Server for Reporting Services (SSRS) and Crystal Reports to generate reports. However if you will only use SSRS, do not select this check box option.
9. The **Report App Server** field displays the name of the application server that handles report tasks for this Web Access extension. If Crystal Reports is installed on a different server, change this application server value to the server you use to generate Crystal Reports.
10. Optionally, update the **NLB Report Repository** location. This field specifies the Network Load Balancing (NLB) report repository location. This shared repository can be accessed by other EWA installations. Either enter this path directly or click the **Browse (...)** button to find and select it.
11. The **Current Deployment** section details the state of the Web Access extension. Review the information in these fields:
  - a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
  - b. **Installed On** - Displays the date on which the current extension version was installed.
  - c. **Server** - Contains the name of the server on which the Web Access extension is installed.
  - d. **Version** - Displays the version number for the extension. Use this value to compare against the current extension version available from Epicor; if you have an older version, consider updating the Web Access extension.

- e. **Extension URL** - Displays the internet website for the Web Access extension. You can click the **Copy URL** button to place this internet website on your clipboard; you could then paste this URL value in other programs and documents as you need.

**12.** When you finish updating the Web Access extension fields, click **Deploy**.

- a. If you receive error messages, update the fields with correct values and click **Deploy** again.
- b. If a Web Access extension on a different application server uses the same virtual directory, you are asked if you want to overwrite it. If you decide to overwrite this directory, the extension will use the current application server and no longer run from its original application server. If you do not overwrite this virtual directory, you receive a validation error and the deployment process stops.
- c. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

A green **Installed** status indicator displays on the sheet. The Web Access extension is now added to your Epicor ERP environment.



**Important** After you deploy the Web Access extension and then later attempt to launch the Application Server Settings program through Windows Explorer, you may receive either a verification error or an assembly error. This occurs because you are accessing this program from the wrong directory. When you launch this program from a `\localhost\<ShareName>` directory, Windows Intranet Security stops the program from running. Instead, navigate to the actual folder location that contains the `SetupEnvironment.exe` file, such as `C:\Users\Administrator\Downloads\Shared\EpicorSetup\SetUpEnvironment`. The program launches as expected.

## Mobile Access

Epicor Mobile Access extends the Epicor Everywhere Framework™ to generate properly sized Web forms for mobile platforms including Windows, iOS and Android.

Since the mobile dashboards that support Epicor Mobile Access (EMA) are built using the dashboard technology and Updatable BAQ technology embedded in the Epicor ERP application, users can create web applications that implement business functionality on mobile devices.

You can have multiple instances of the Epicor Mobile Access extension linked to each application server.

- 1.** You use this sheet to install a new Mobile Access extension or add an existing extension. You can also update a Mobile Access extension so it connects properly with the current system.
  - a. To update an existing extension, click the **Existing Deployment** drop-down list to select which Mobile Access extension you need to review or update.
  - b. To install a new extension, click the **New** button.  
The fields on the Mobile Access sheet activate for data entry.
  - c. To add an existing extension, click the **Browse** (...) button.  
The Application Server Settings program locates existing Mobile Access extensions; select the extension you wish to add. After you select the Mobile Access extension, the fields activate for data entry.
- 2.** If you need, enter the **Deployment Name** for this Mobile Access extension. Be sure to enter a name that helps you identify each Mobile Access extension available on your system.
- 3.** Select the **Install Version** for the Mobile Access extension. The available versions display on this drop-down list; select the version that matches the new installation or update.

4. Now define the **Install Path** for the Mobile Access extension. If you need, click the **Browse (...)** button to find and select this folder. The default install path is **\inetpub\wwwroot**.
5. Enter your site name in the **Web Site** field. The default value for this field is **Default Web Site**.
6. The **Virtual Directory** field displays the default name for the Epicor Mobile Access extension folder. You can change this value to any name that Internet Information Services (IIS) will accept. After you deploy the Mobile Access extension, a virtual directory is created in IIS using a physical path and the folder you define in this field. This physical path will be the **Install Path** directory.
7. By default the **Application Pool Name** uses the value you entered in the **Application Name** field on the **Application Server > Application Server Settings** sheet. You cannot change this value; it defines the name of the application pool associated with the application server hosting the Mobile Access extension. An application pool defines a group of related URLs that use the same process or set of processes. The new application server must be placed in an application pool.

Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.

If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the LocalSystem account. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account.
8. If you need to enter a specific user account for the Internet Information Services (IIS) application pool this application server uses, select the **Use Custom Account** check box.
9. The **Current Deployment** section details the state of the Mobile Access extension. Review the information in these fields:
  - a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
  - b. **Installed On** - Displays the date on which the current extension version was installed.
  - c. **Server** - Contains the name of the server on which the Mobile Access extension is installed.
  - d. **Version** - Displays the version number for the extension. Use this value to compare against the current extension version available from Epicor; if you have an older version, consider updating the Mobile Access extension.
  - e. **Extension URL** - Displays the internet website for the Mobile Access extension. You can click the **Copy URL** button to place this internet website on your clipboard; you could then paste this URL value in other programs and documents as you need.
10. When you finish updating the Mobile Access extension fields, click **Deploy**.
  - a. If you receive error messages, update the fields with correct values and click **Deploy** again.
  - b. If a Mobile Access extension on a different application server uses the same virtual directory, you are asked if you want to overwrite it. If you decide to overwrite this directory, the extension will use the current application server and no longer run from its original application server. If you do not overwrite this virtual directory, you receive a validation error and the deployment process stops.
  - c. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

A green **Installed** icon displays on the sheet. The Mobile Access extension is now added to your Epicor ERP environment.



**Important** After you deploy the Mobile Access extension and then later attempt to launch the Application Server Settings program through Windows Explorer, you may receive either a verification error or an assembly error. This occurs because you are accessing this program from the wrong directory. When you launch this program from a `\localhost<ShareName>` directory, Windows Intranet Security stops the program from running. Instead, navigate to the actual folder location that contains the `SetupEnvironment.exe` file, such as `C:\Users\Administrator\Downloads\Shared\EpicorSetup\SetUpEnvironment`. The program launches as expected.

## Enterprise Search

Enterprise Search is a powerful search application which you can use to retrieve indexed content from within your Epicor ERP application and then quickly launch specific programs to display the data returned from the search.

Using the default search index definition shipped with Epicor ERP, you can search on any item within the Epicor database - like a part, customer, purchase order, AR invoice, and so on. All the records within the Epicor database that use this record in some way appear within the search results. Results are organized by record type and can be filtered by record type.

You can only have one instance of the Enterprise Search extension linked to each application server.

1. You use this sheet to install a new Enterprise Search extension or add an existing extension. You can also update the current Enterprise Search extension.
  - a. To install a new Enterprise Search extension, click the **New** button. Enter the **Deployment Name** for this Enterprise Search extension. Be sure to enter a name that helps you identify each Enterprise Search extension available on your system.  
The fields on the Enterprise Search sheet activate for data entry.
  - b. To add an existing Enterprise Search extension, click the **Browse (...)** button. The Application Server Settings program locates existing Enterprise Search extensions; select the extension you wish to add or update. After you select the Enterprise Search extension, the fields activate for data entry.
  - c. To update the Enterprise Search extension, enter the new values in the fields on this sheet.
2. Enter an **SSL Certificate Subject Name** or click the **Browse (...)** button to find and select it. Enterprise Search connects to the server over HTTPS and requires specifying a valid Secure Sockets Layer (SSL) Certificate issued by the Epicor server. Please refer to the **Add Epicor Application Server** topic for more information on SSL Certificates.
3. Enter the **Server Name** for the database server that contains the database you will use with this Enterprise Search database.
4. Now click the **Authentication** drop-down list and select either the **Windows Authentication** or **SQL Server Authentication** option.
  - a. If you select Windows Authentication, the **User** and **Password** default to your current login values and these fields are disabled.
  - b. If you select SQL Server Authentication, enter the User and Password you use to log into SQL Server.

5. Now from the **Database Name** drop-down list, select the name of the SQL database you will link to this Enterprise Search database. You can find this name on the **Application Server > Database Connection** sheet.

6. If you are setting up Enterprise Search for the first time, select the **Create DB** check box. When you select this option and click **OK**, a new database generates using the name you entered in the **Server Name** field. If you update the Enterprise Search settings later, you can select this database again or if needed, create a new database.

When you save, this database is validated. If the Application Server Setup program cannot find this database in the location you specified, an error message displays.

Note that when you register an existing Enterprise Search database, you cannot create a new database. If you wish to create a new Enterprise Search database for an existing application server, you must reconfigure it. To do this, navigate to the **Application Server > Database Connection** sheet. Enter a new **Server Name** on this sheet. Then return to the Extensions > Enterprise Search sheet, enter this **Server Name** and select the **Create DB** check box; after you click **OK** the new Enterprise Search database generates.

7. To verify the application server can connect with this Enterprise Search database, click **Test Connection** and click **OK** in the confirmation message.

8. A dialog box displays indicating the test was successful. Click **OK**.

9. In the **Service Account** section, enter the credentials for the user identity that will run the Epicor Search Indexer service:

- a. For the **Built In Account**, use the drop-down arrow to select your type of account, typically **Custom Account**.
- b. If you selected a **Custom Account**, enter the **User** and **Password** for the custom account you wish to use.

10. The **Current Deployment** section details the state of the Enterprise Search extension. Review the information in these fields:

- a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
- b. **Installed On** - Displays the date on which the current extension version was installed.
- c. **Server** - Contains the name of the server on which the Enterprise Search extension is installed.
- d. **Version** - Displays the version number for the extension. Use this value to compare against the current version available from Epicor; if you have an older version, consider updating the Enterprise Search extension.

11. Click the **Create Search Index** button to generate an index of your database. When users initiate an Enterprise Search, the search function calls this index to locate database records that match your search criteria. Values from this index populate the Enterprise Search results.

12. When you finish updating the Enterprise Search extension fields, click **Deploy**.

- a. If you receive error messages, update the fields with correct values and click **Deploy** again.
- b. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

A green **Installed** icon displays on the sheet. The Enterprise Search extension is now added to your Epicor ERP environment.



**Important** After you deploy the Enterprise Search extension and then later attempt to launch the Application Server Settings program through Windows Explorer, you may receive either a verification error or an assembly error. This occurs because you are accessing this program from the wrong directory. When you launch this program from a \\localhost\\<ShareName> directory, Windows Intranet Security stops the program from running. Instead, navigate to the actual folder location that contains the SetupEnvironment.exe file, such as **C:\Users\Administrator\Downloads\Shared\EpicorSetup\SetUpEnvironment**. The program launches as expected.

## Epicor Education

Epicor's library of embedded educational materials provides you with a platform for developing an effective training program for your organization. The number of resources enable you to choose the best options to meet your training needs and tailor the content to fit your users.

You install the Embedded Courses on the Epicor Education sheet. You can only have one instance of the Epicor Education extension linked to each application server.



**Important** Verify that the ASP.NET module of your Windows Internet Information Services (IIS) installation is enabled before you install the embedded courses.

1. You use this sheet to install a new Epicor Education extension or add an existing extension. You can also update the current Epicor Education extension.
  - a. To install a new Epicor Education extension, click the **New** button. The fields on the Epicor Education sheet activate for data entry.
  - b. To add an existing Epicor Education extension, click the **Browse (...)** button. The Application Server Settings program locates existing Epicor Education extensions; select the extension you wish to add or update. After you select the Epicor Education extension, the fields activate for data entry.
  - c. To update the Epicor Education extension, enter the new values in the fields on this sheet.
2. If you need, enter the **Deployment Name** for this Epicor Education extension. Be sure to enter a name that helps you identify each Epicor Education extension available on your system.
3. Now define the **Install Path** for the Embedded Education courses. This indicates the location for the source files that display course content in the Epicor ERP application.
4. Enter your site name in the **Web Site** field. If you do not have a name you wish to use, accept the Default Web Site value.
5. The **Virtual Directory** field displays the default name for the Epicor Education extension folder. You can change this value to any name that Internet Information Services (IIS) will accept. After you deploy the Epicor Education extension, a virtual directory is created in IIS using a physical path and the folder you define in this field. This physical path will be the **Install Path** directory.
6. By default the **Application Pool Name** uses the value you entered in the **Application Name** field on the **Application Server > Application Server Settings** sheet. You cannot change this value; it defines the name of the application pool associated with the application server hosting the Epicor Education extension. An application pool defines a group of related URLs that use the same process or set of processes. The new application server must be placed in an application pool.

- 7.** If you need to enter a specific user account for the Internet Information Services (IIS) application pool the Epicor Education extension uses, select the **Use Custom Account** check box.

Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.

If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the LocalSystem account. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account.

- 8.** The **Current Deployment** section details the state of the Epicor Education extension. Review the information in these fields:

- a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
- b. **Installed On** - Displays the date on which the current extension version was installed.
- c. **Server** - Contains the name of the server on which the Epicor Education extension is installed.
- d. **Version** - Displays the version number for the extension. Use this value to compare against the current extension version available from Epicor; if you have an older version, consider updating the Epicor Education extension.
- e. **Extension URL** - Displays the internet website for the Epicor Education extension. You can click the **Copy URL** button to place this internet website on your clipboard; you will use this value later to connect a company with the embedded courses.

- 9.** When you finish updating the Epicor Education extension fields, click **Deploy**.

- a. If you receive error messages, update the fields with correct values and click **Deploy** again.
- b. If an Education extension on a different application server uses the same virtual directory, you are asked if you want to overwrite it. If you decide to overwrite this directory, the extension will use the current application server and no longer run from its original application server. If you do not overwrite this virtual directory, you receive a validation error and the deployment process stops.
- c. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

A green **Installed** icon displays on the sheet. The Epicor Education extension is now added to your Epicor ERP environment.

- 10.** You next need to connect the company to the Epicor Education URL. To do this, copy the Extension URL value.

- 11.** Launch the **Epicor ERP** application.

- 12.** Navigate to **Company Maintenance**.

**Menu Path:** System Setup > Company/Site Maintenance > Company Maintenance



**Important** This program is not available in Epicor Web Access.

- 13.** On the **General Settings** tab, paste the Extension URL you copied into the **Education Courses URL** field.

- 14.** Click **Save**.

Users in the current company can now launch the embedded courses. If you need, launch Company Maintenance in other companies and paste the Education Courses URL as needed. Users in these companies can then access the Epicor Education courses.



**Important** After you deploy the Epicor Education extension and then later attempt to launch the Application Server Settings program through Windows Explorer, you may receive either a verification error or an assembly error. This occurs because you are accessing this program from the wrong directory. When you launch this program from a \\localhost\\<ShareName> directory, Windows Intranet Security stops the program from running. Instead, navigate to the actual folder location that contains the SetupEnvironment.exe file, such as C:\\Users\\Administrator\\Downloads\\Shared\\EpicorSetup\\SetUpEnvironment. The program launches as expected.

## Information Worker

Information Worker connects the Epicor ERP data with Microsoft® Office® applications. Through this application, users have direct access to Epicor ERP from inside Microsoft Outlook®, Word®, and Excel®.

You can only have one instance of the Information Worker extension linked to each application server.

1. You use this sheet to install a new Information Worker extension or add an existing extension. You can also update the current Information Worker extension.
  - a. To install a new Information Worker extension, click the **New** button. The fields on the Information Worker sheet activate for data entry.
  - b. To add an existing Information Worker extension, click the **Browse (...)** button. The Application Server Settings program locates existing Information Worker extensions; select the extension you wish to add or update. After you select the Information Worker extension, the fields activate for data entry.
  - c. To update the Information Worker extension, enter the new values in the fields on this sheet.
2. If you need, enter the **Deployment Name** for this Information Worker extension. Be sure to enter a name that helps you identify each Information Worker extension available on your system.
3. Now define the **Install Path** for the Information Worker extension. This indicates the location for the files that connect the Epicor ERP data to the Microsoft Office applications.
4. Enter your site name in the **Web Site** field. If you do not have a name you wish to use, accept the Default Web Site value.
5. The **Virtual Directory** fields displays the default name for the Information Worker extension directory. You can change this value to any name that Internet Information Services (IIS) will accept. After you deploy the Information Worker extension, a virtual directory is created in IIS using a physical path and the folder you define in this field. This physical path will be the **Install Path** directory.
6. By default the **Application Pool Name** uses the value you entered in the **Application Name** field on the **Application Server > Application Server Settings** sheet. You cannot change this value; it defines the name of the application pool associated with the application server hosting the Information Worker extension. An application pool defines a group of related URLs that use the same process or set of processes. The new application server must be placed in an application pool.
7. If you need to enter a specific user account for the Internet Information Services (IIS) application pool the Information Worker extension uses, select the **Use Custom Account** check box.

Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.

If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the LocalSystem account. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account.

8. Now use the fields in the **E-Mail Error Settings** group box to indicate how Information Worker handles errors that appear in the Microsoft® Office Suite®. When users receive errors in an Office Suite program, they have the option to report these errors to their administrator. Use these fields to set up who should receive these error messages. Define these values:
  - a. **E-Mail Address** - Enter the e-mail address for the administrator who will receive the error messages.
  - b. **E-Mail Subject** - Enter the default text that will display in the **Subject** field for the e-mail message. Be sure to enter text that clearly identifies the source of the e-mail message.
- When users send a Microsoft Office Suite error message to their administrator, the error displays in the body of the e-mail message.
9. The **Current Deployment** section details the state of the Information Worker extension. Review the information in these fields:
  - a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
  - b. **Installed On** - Displays the date on which the current extension version was installed.
  - c. **Server** - Contains the name of the server on which the Information Worker extension is installed.
  - d. **Version** - Displays the version number for the extension. Use this value to compare against the current extension version available from Epicor; if you have an older version, consider updating the Information Worker extension.
  - e. **Extension URL** - Displays the internet website for the Information Worker extension. You can click the **Copy URL** button to place this internet website on your clipboard; you could then paste this URL value in other programs and documents as you need.
10. When you finish updating the Information Worker extension fields, click **Deploy**.
  - a. If you receive error messages, update the fields with correct values and click **Deploy** again.
  - b. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.



**Important** After you deploy the Information Worker extension and then later attempt to launch the Application Server Settings program through Windows Explorer, you may receive either a verification error or an assembly error. This occurs because you are accessing this program from the wrong directory. When you launch this program from a \\localhost\\<ShareName> directory, Windows Intranet Security stops the program from running. Instead, navigate to the actual folder location that contains the SetupEnvironment.exe file, such as **C:\Users\Administrator\Downloads\Shared\EpicorSetup\SetUpEnvironment**. The program launches as expected.

## Epicor Help

The Epicor application help contains the documentation users need to run the Epicor application. Use this sheet to install and update the application help.



**Note** Before you deploy the application help, make sure the Windows Search service is installed and running.

The application help has detailed descriptions of each program, process, and report within the Epicor application. It also contains user guides that give users step-by-step instructions for these programs and processes. Additionally technical references guides are embedded in the application help, providing users the ability to search on specific content or display each technical reference guide as a standalone .pdf file.

You can have multiple instances of the Epicor Help extension linked to each application server.

1. You use this sheet to install an instance of the Epicor application help or update an existing application help instance.
  - a. To update an existing extension, click the **Existing Deployment** drop-down list to select which application help extension you need to review or update.
  - b. To install the application help, click the **New** button.  
The fields on the Epicor Help sheet activate for data entry. Enter the **Deployment Name** for this application help release. Be sure to enter a name that helps you identify the specific Epicor Help release on your system.
  - c. To update the application help with a new release, click the **Browse (...)** button.  
The Application Server Settings program locates existing application help releases; select the release you wish to update. After you select the application help release you want to update, the fields activate for data entry.
2. Now enter the **Install Path** for the application help release. This indicates the location where the files will be placed when you deploy the application help.
3. The **Full Path** to the application help displays for your information. This value indicates where the application help installs within the Epicor application directory. Notice this directory path includes the **Install Path** plus the **\Epicor10Help** folder.
4. Enter your site name in the **Web Site** field. If you do not have a name you wish to use, accept the Default Web Site value.
5. The **Virtual Directory** field displays the default name for this application help release folder. You can change this value to any name that Internet Information Services (IIS) will accept. After you deploy the application help extension, a virtual directory is created in IIS using a physical path and the folder you define in this field. This physical path will be the **Full Path** directory.
6. Enter a **Session Timeout (minutes)** value. This time limit threshold indicates how long the application help window can remain open before the system shuts down the current session.
7. By default the **Application Pool Name** uses the value you entered in the **Application Name** field on the **Application Server > Application Server Settings** sheet. You cannot change this value; it defines the name of the application pool associated with the application server hosting the application help.  
An application pool defines a group of related URLs that use the same process or set of processes. The new application server must be placed in an application pool.

8. If you need to enter a specific user account for the Internet Information Services (IIS) application pool that the application help uses, select the **Use Custom Account** check box.

Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.

If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the LocalSystem account. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account.

9. The **Current Deployment** section details the state of the application help. Review the information in these fields:

- a. **Status Indicator** - This icon indicates whether the application help is **Not Installed** (red) or **Installed** (Green).
- b. **Installed On** - Displays the date on which the current help release was installed.
- c. **Server** - Contains the name of the server on which the application help is installed.
- d. **Version** - Displays the version number for the application help release. Use this value to compare against the current application help available from Epicor; if you have an older version, consider updating the application help release.
- e. **Extension URL** - Displays the internet website for the application help. You can click the **Copy URL** button to place this internet website on your clipboard; you could then paste this URL value in other programs and documents as you need.

10. When you finish updating the Epicor Help fields, click **Deploy**.

- a. If you receive error messages, update the fields with correct values and click **Deploy** again.
- b. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.



**Important** After you deploy the application help and then later attempt to launch the Application Server Settings program through Windows Explorer, you may receive either a verification error or an assembly error. This occurs because you are accessing this program from the wrong directory. When you launch this program from a \\localhost\\<ShareName> directory, Windows Intranet Security stops the program from running. Instead, navigate to the actual folder location that contains the SetupEnvironment.exe file, such as **C:\Users\Administrator\Downloads\Shared\EpicorSetup\SetUpEnvironment**. The program launches as expected.

## Data Discovery

Epicor Data Discovery (EDD) is a Business Intelligence solution intended to provide an extremely easy to use sense-making, data exploration, data visualization experience. EDD is a major component of the overall Epicor Data Platform which encompasses a broad set of capabilities for managing, accessing, sharing, cleansing, visualizing, and extracting insights from data created by or related to Epicor created data.

Use these steps to install Epicor Data Discovery.

1. Prior to installing the Data Discovery extension, configure Token Authentication. First, you need to set up Data Discovery to use the Epicor ERP account:



**Note** Token Authentication is configured automatically during application server deployment. Use these steps if you have issues with automatic configuration and need to run the process manually.

- a. In Epicor Administration Console, in the tree view, expand your Epicor ERP server node.
- b. In the **Actions** pane, click **Configure Token Authentication**.
- c. In the **Token Authentication Settings** dialog box, select the **Enable Token Authentication** checkbox
- d. In the **Lifetime (sec):** field, set the token lifetime greater than 0, and click **Generate** to create the **Sign Key**.

**2.** Verify the following fields:

- a. In the Admin Console, right-click on your Application Server and select **Application Server Configuration**. Select the **Application Server > Application Server Setup** tab.
- b. Verify that the **Https Endpoint Binding** field is set to **HttpBinaryWindowsChannel**.
- c. Click **OK**.

**3.** Select the **Epicor Data Discover** tab.

**4.** To install a new instance of the Epicor Data Discovery or upgrade an existing Epicor Data Discovery instance, choose one of the following:

- a. To install a new extension, click the **New** button. Enter the **Deployment Name** for this Epicor Data Discovery instance. Be sure to enter a name that helps you identify each Epicor Data Discovery extension available on this application server.
- b. To update an existing extension, click the **Existing Deployment** drop-down list to select which Epicor Data Discovery extension you need to review or update.
- c. To add an existing extension, click the **Browse (...)** button. The Application Server Settings program locates existing Epicor Data Discovery extensions. Select the extension you wish to add. After you select the Data Discovery extension, the fields activate for data entry.

**5.** If you have the **Advanced Epicor Data Discovery** license, enter the **License File** to identify your company's license for Epicor Data Discovery. If you do not enter a license file, only the Epicor Data Discovery basic functionality will be installed.

For more information on EDD licenses, refer to the Licensing Administrative Overview topic in the Epicor Data Discovery help.

**6.** In the **SSL Qualified Domain Name** field, you must enter the SSL domain name for the Epicor ERP server that will connect to Epicor Data Discovery.

**7.** Define the Application Pool details:

- a. In the **Application Pool Name** field, select the Application Pool that will be used by the Epicor Web Access application. The drop-down list displays only the application pools that are set to use Integrated Pipeline mode. If the list is empty, click the New button to create a new application pool that uses an Integrated pipeline.
- b. If you want to use a custom account, select the **Use Custom Account** check box and enter **Application Pool Username** and **Application Pool Password** for the account.

8. From the **Built In Account** drop-down, select an account to run the Application Pool. You can select either a built-in account that runs through the **ApplicationPoolIdentity**, **LocalSystem**, **LocalService**, or **NetworkService**, or select the **Specific User** option to define a custom account.
9. Selecting the **Specific User** built-in account activates the **Application Pool Username** and **Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.
10. Enter the **Server Name** for the database server that contains the database you will use with this Data Discovery database or accept the default value.
11. Now click the **Authentication** drop-down list and select either the **Windows Authentication** or **SQL Server Authentication** option.
  - a. If you select Windows Authentication, the **User** and **Password** default to your current login values and these fields are disabled.
  - b. If you select SQL Server Authentication, enter the **User** and **Password** you use to log into SQL Server.
12. Now from the **Database Name** drop-down list, select the name of the SQL database you will link to this Data Discovery database or accept the default name.
13. To verify the application server can connect with this Data Discovery database, click **Test Connection** and click **OK** in the confirmation message.
14. A dialog box displays indicating the test was successful. Click **OK**.
15. Use the ERP Admin Account section to enter your Epicor User Name and Password which will be used to login to this Epicor Data Discovery instance.
16. The **Current Deployment** section details the state of the Data Discovery extension. Review the information in these fields:
  - a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
  - b. **Installed On** - Displays the date on which the current extension version was installed.
  - c. **Server** - Contains the name of the server on which the Data Discovery extension is installed.
  - d. **Version** - Displays the version number for the extension. Use this value to compare against the current extension version available from Epicor; if you have an older version, consider updating the Data Discovery extension.
  - e. **Extension URL** - Displays the internet website for the Data Discovery extension. You can click the **Copy URL** button to place this internet website on your clipboard; you could then paste this URL value in other programs and documents as you need.
17. When you finish updating the Data Discovery extension fields, click **Deploy**.
  - a. If you receive error messages, update the fields with correct values and click **Deploy** again.
  - b. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

- 18.** Click the **Deploy** button. The Deployment Status window displays a progress bar as it validates the deployment process. When finished, click **Close**.
- If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.
  - If you receive error messages, update the fields with correct values and click **Deploy** again.
  - If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

A green **Installed** icon displays on the sheet. The Data Discovery extension is now added to your Epicor ERP environment.

## Web Configurator

Epicor Web Configurator is a web based client for the Configurator. You can use it to work with the Dealer Portal that links manufacturers directly with dealers. This functionality is designed for manufacturers who sell configured products through a distributor or dealer channel. By receiving transactions from dealers through the Dealer Portal, these manufacturers sell their products, track products after they ship them, and support warranty and repair needs.

- To deploy Web Configurator you must hold the **Advanced Configurator** license.
- Verify that the **ASP.NET** module of your Windows Internet Information Services (IIS) installation is enabled before you start to install Web Configurator.
- Create/Use an App Pool running as **LocalSystem**.
- **Install Node JS** - required to install Angular CLI. You may download the Node.js from here: <https://nodejs.org/en/download>
- **Install Angular CLI** - it may be installed using the following NPM command: `npm install -g @angular/cli`

NPM is part of the nodejs installation. For more information about Angular CLI, visit <https://cli.angular.io/>

- 1.** You use this sheet to install a new Web Configurator extension or add an existing extension. You can also update a Web Configurator extension so it connects properly with the current system.
  - a. To update an existing extension, click the **Existing Deployment** drop-down list to select which Web Configurator extension you need to review or update.
  - b. To install a new extension, click the **New** button.  
The fields on the Web Configurator sheet activate for data entry.
  - c. To add an existing extension, click the **Browse** (...) button.  
The Application Server Settings program locates existing Web Configurator extensions; select the extension you wish to add. After you select the Web Configurator extension, the fields activate for data entry.
- 2.** If you need, enter the **Deployment Name** for this Web Configurator extension. Be sure to enter a name that helps you identify each Web Configurator extension available on your system.
- 3.** Enter your Web Configurator site name in the **Web Site** field. If you do not have a name you wish to use, accept the Default Web Site value.
- 4.** The **Virtual Directory** field displays the default name for the Web Configurator extension folder. The name can be changed to any name allowed in IIS. After you deploy the Web Configurator extension, a virtual directory is created in IIS using a physical path and the folder you define in this field. This physical path will be the **Install Path** directory.

5. By default the **Application Pool Name** uses the value you entered in the **Application Name** field on the **Application Server > Application Server Settings** sheet. You cannot change this value; it defines the name of the application pool associated with the application server hosting the Web Configurator extension. An application pool defines a group of related URLs that use the same process or set of processes. The new application server must be placed in an application pool.

6. If you need to enter a specific user account for the Internet Information Services (IIS) application pool the Web Configurator extension uses, select the **Use Custom Account** check box.

Selecting this check box activates the **Application Pool Username** and **Application Pool Password** fields. Enter the domain and the user account in the Application Pool Username field; for example, enter MyDomain\UserName. To effectively connect with the server, this account must be a valid domain account with access rights to the network. If this account is not valid, you will not be able to stop and start the application pool.

If you do not select this check box, the application pool uses a default user account. If you use an SSRS server, the connection uses the LocalSystem account. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account.

7. The **Current Deployment** section details the state of the Web Configurator extension. Review the information in these fields:

- a. **Status Indicator** - This icon indicates whether the extension is **Not Installed** (red) or **Installed** (Green).
- b. **Installed On** - Displays the date on which the current extension version was installed.
- c. **Server** - Contains the name of the server on which the Web Configurator extension is installed.
- d. **Version** - Displays the version number for the extension. Use this value to compare against the current extension version available from Epicor; if you have an older version, consider updating the Web Configurator extension.
- e. **Extension URL** - Displays the internet website for the Web Configurator extension. You can click the **Copy URL** button to place this internet website on your clipboard; you will use this value later to connect a company with the web configurator functionality.

8. When you finish updating the Web Configurator extension fields, click **Deploy**.

- a. If you receive error messages, update the fields with correct values and click **Deploy** again.
- b. If an Web Configurator extension on a different application server uses the same virtual directory, you are asked if you want to overwrite it. If you decide to overwrite this directory, the extension will use the current application server and no longer run from its original application server. If you do not overwrite this virtual directory, you receive a validation error and the deployment process stops.
- c. If the application server can connect to the extension, a confirmation dialog displays. Click **OK**.

A green **Installed** icon displays on the sheet. The Web Configurator extension is now added to your Epicor ERP environment.

9. In the Current Deployment section, verify that the **Extension URL** has been updated to include the latest release version. Click the **Copy URL** button to copy the URL into your clipboard.
10. Log into your Epicor ERP 10 application. Open **System Setup > Company / Site Maintenance > Company Configuration**.

11. Navigate to the **Modules > All Modules > General** sheet and paste the copied URL in the **Generator URL** field in the Epicor Web Configurator group. For **Run Time URL**, you can use the same URL or specify your own website.
12. When complete, click **Save**.

## Configure Remote Machines

---

You may need to set up application servers on other machines within your network. This section details tasks you do to configure application servers on these remote machines.

### Remote Connection Setup

If you run an application server from a remote machine, you must activate the Internet Information Services (IIS) Management Service on this remote system.

To activate this service:

1. Log into the remote machine.
2. From the Windows Desktop, click **Start > Control Panel**.  
The Control Panel window displays.
3. Double-click on the **Programs and Features** icon.  
The **Uninstall or change a program** window displays.
4. From the left panel, select the **Turn Windows features on or off** option.
5. After the **Windows Features** dialog box populates with features, expand the **Internet Information Services** node.
6. Now expand the **Web Management Tools** node.
7. Verify the **IIS Management Service** check box is selected. If not, select this check box.
8. Click **OK**.

The IIS Management Service is now active on this remote machine, and the application server should run as expected.

## Add a Task Agent

---

After you set up an application server (AppServer), you can then configure task agents for the database. Task agents handle all scheduled tasks within the Epicor ERP application.

You can set up a maximum of **three** task agents to run against the same database. By setting up multiple task agents, you ensure the Epicor ERP application continues to process tasks when a task agent stops working. If a process does not finish because a task agent stops, the next available task agent picks up the process and it begins running again. For example, if one task agent stops because the server it is running on shuts down, another task agent can continue to process the tasks in the queue.

To properly configure this redundancy for your system, these multiple task agents must be created on different machines. Each schedule automatically has a two minute limit. If the schedule is not processed in two minutes, the next available task agent picks up the schedule and the process restarts.

To create a task agent, launch the **Task Agent Service Configuration for X.X.X.** program (Where X.X.X. is the ICE version installed with the service) from Admin Console. Use this program to add task agents that run on either a local machine or a remote machine.

Note that you can install multiple versions of the Task Agent Service Configuration on the same server. Each version of the service has the ICE version number appended at the end of the program title. For example, you can have both Task Agent Service Configuration for 3.2.300 and Task Agent Service Configuration for 3.2.400 installed on the same machine. Through this feature, you can have multiple versions of the service running at the same time when you have different versions of AppServer installed on the same machine. In the control panel, each instance of the service displays as a separate icon identified by its version number.

In the Epicor ERP application, the task agent activates the programs added to recurring schedules. Users add programs to recurring schedules through the **Schedule** drop-down lists available on programs throughout the Epicor ERP application. These schedules can be set up in the Epicor ERP application using **System Agent Maintenance**.

## Remote Firewall Setup

When you run the task agent on a remote machine and this machine uses a firewall, be sure **Port 9010** is open. If this port is not open, you cannot administrate the task agent through the Epicor Administration Console.

1. On your server, launch **Windows Firewall with Advanced Security**.
2. From the tree view, select the **Inbound Rules** node.
3. Click on the **Action > New Rule...** option.
4. The **New Inbound Rule Wizard** displays. Select **Port**.
5. Click **Next**.
6. The **Protocol and Ports** pane displays. Enter the following values:
  - a. Select the **TCP** option.
  - b. Select the **Specific Local Ports** option.
  - c. In the **Port** field, enter **9010**.
7. Click **Next**. The **Actions** pane displays.
8. Select the **Allow the Connection** option.
9. Click **Next**. The **Profile** sheet displays.
10. Clear the **Public** check box.
11. Click **Next**. The **Name** sheet displays.
12. Enter an appropriate **Name** and **Description** for the new inbound rule.
13. Click **Finish**.

## Launch Task Agent Service Configuration

Depending on how you install the Task Agent Service Configuration program, you launch this program in different ways.

When you install the **Task Agent Service**, the Task Agent Service Configuration program is placed in the following Start menu path. You launch the program directly from this location.

- **Start > All Programs > Epicor Software > Epicor Administration Tools > Task Agent Service Configuration for X.X.X.X > Task Agent Service Configuration** (Where X.X.X.X is the ICE version installed with the service)

This program is also included as part of the **Epicor Administration Console** installation. When you install the Task Agent Service Configuration program in this way, it does not appear on the Start menu. Instead, you launch this program through the Epicor Administration Console. To do this:

1. From the tree view, select the application server that contains the task agent you wish to modify.
2. Now on the **Actions** pane, click the **Connect to Application Server** button.
3. After you connect to the application server, the **Task Agent Configuration** button displays on the **Details** sheet. Click this button. If the task agent is not installed, do the following:
  - a. You are asked if you want to install the task agent now; click **Yes**.  
The task agent installer runs. When the installation is complete, the **Task Agent Configuration** window displays.
  - b. You can now create the task agent. Click **File > New Task Agent**.
  - c. The **Add New Task Agent** window displays, using the default values from the application server. Create the task agent.
4. When a task agent is available, you may need to enter your **User Name** and **Password**. You may also be prompted to enter these values twice; once to connect with the WCF service, and again when connecting to the **Service Controller**.

The **Task Agent Service Configuration for X.X.X.X** (Where X.X.X.X is the ICE version installed with the service) window displays. The values defined for the current task agent display on the window.

 **Tip** If the task agent service is not running or the Epicor Administration Console cannot communicate with the service, the configuration information does not display. Several menu options are also disabled. Likewise, if you click on the Actions menu and select Stop Service, the same fields and menu options are disabled.

## Create a New Task Agent

You can create a new task agent from the Task Agent Service Configuration program. To do this:

1. Click on **File > New Task Agent**.  
The **Add Task Agent** window displays. If you need more information about a specific field on this window, review the **Task Agent Fields** topic.
2. Enter the unique **Name** for this task agent. Enter a value that helps you easily identify the task agent later.
3. Verify the **Enabled** check box is selected.

4. Indicate the **AppServer URL** that connects the task agent to the application server (AppServer).



**Tip** You can find this value by opening the system configuration file for the client installation. Locate the **AppServerURL** node and copy this value.

5. Now define the **Endpoint Binding** type this task agent will use. This value defines how this application server checks for authentication certificates through Internet Information Services (IIS). When a user logs into the application, the selected method checks whether the user can access the Epicor application.



**Tip** To learn how to access this service and enter this account, review the **Windows Endpoint Configuration** topic. For more information on how you set up each authentication method, review either the **Epicor 10 Architecture Guide** or the **System Administration Guide**.

Available options:

- **UsernameWindowsChannel** - This NET.TCP binding authenticates transactions through an Epicor Username and Password. Windows checks for existing Epicor user accounts to authenticate logins.
- **UsernameSSLChannel** - This NET.TCP binding authenticates transactions using a Secure Sockets Layer (SSL) X509 certificate. Leverage this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor application.

Selecting this option causes the **SSL Certificate Subject Name** and **DNS Endpoint Identity** fields to appear. You use these fields to enter the name of your SSL certificate and the identity of the server.

- **Windows** - This NET.TCP binding authenticates transactions using a Windows Username and Password. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.
- **HttpBinaryUsernameSslChannel** - This HTTP binding protocol authenticates using a Secure Sockets Layer (SSL) X509 certificate. The data transfers between the client and server using Hypertext Transfer Protocol (HTTP). Instead of the transport, the message which contains the data transfer is encrypted. Because this binding does not use Hypertext Transfer Protocol Secure (HTTPS), it tends to be slower than bindings which use HTTPS.

Use this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor ERP application.

Selecting this option causes the SSL Certificate Subject Name and DNS Endpoint Identity fields to appear. You use these fields to enter the name of your SSL certificate and the identity of the server.

- **HttpsBinaryUsernameChannel** - This HTTPS binding authenticates transactions using an Epicor Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). HTTPS encrypts the data transfer.
- **HttpsBinaryWindowsChannel** - This HTTPS binding authenticates transactions using a Windows Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

You can select this method for application servers that handle smart client installations and Epicor Web Access (EWA) installations where users access the application through the same domain. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.

- **HttpsOffloadbinaryUserNameChannel** - This HTTPS protocol binding is a configuration that offloads encryption handling to an intermediary Application Request Router such as an F5.

The binding authenticates using an Epicor Username and Password token. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

- **HttpsOffloadBinaryAzureChannel** - This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an intermediary Application Request Router such as an F5.

The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Azure AD. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

 **Important** When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the **AddressFilterModeAny** node in web.config as shown below:

```
Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens
```

```
<AddressFilterModeAny />
```

- **HttpsOffloadBinaryIdpChannel** - This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an intermediary Application Request Router such as an F5.

 **Important Epicor Identity Provider** is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available **internally** to Epicor.

The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Epicor Identity Provider deployment. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.

 **Important** When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the **AddressFilterModeAny** node in web.config as shown below:

```
Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens
```

```
<AddressFilterModeAny />
```

- **HttpsBinaryAzureChannel** - Use this protocol to enable authentication of ERP application users against users in Microsoft Azure Active Directory (Azure AD).

This binding relies upon the user authenticating against Azure Active Directory and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

- **HttpsBinaryIdpChannel** - Use this protocol to enable authentication of ERP application against Epicor Identity Provider (IdP).

 **Important Epicor Identity Provider** is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available **internally** to Epicor.

This binding relies upon the user authenticating against IdP and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).

6. If you use **UsernameWindowsChannel**, **UsernameSSLChannel**, or the **HttpsBinaryUsernameSslChannel** endpoint binding, enter the **User ID** and **User Password** for the account. Enter a valid ICE or Epicor user account identifier in these fields.

 **Tip** You should create a special ICE Manager account that has access to all companies and has session impersonation rights. You create this account in **User Account Security Maintenance**. You activate impersonation rights on the **Options** sheet; select the **Allow System Impersonation** check box.

You add companies to the user account through this program as well. For more information on User Account Security Maintenance, review the Epicor application help.

Typically this account should also be selected on the system agent in **System Agent Maintenance**. If you use a different user account on the system agent, make sure it can access all companies and sites, as this account runs processes like MRP and scheduling.

**7.** If you use **HttpsBinaryIdPChannel** or **HttpsOffloadBinaryIdPChannel**, enter the following values:

- **Identity Provider App ID** - enter the ClientID/GUID of an IdP application used to authenticate inter-server communication processes. The application needs to have the following attributes:

Type	Client Claim
Inter-server communication	email - specify IdP user mapped to Epicor ERP user's External Identity.

- **Identity Provider App Secret** - specify the application secret value.

 **Tip** For ERP user, you should create a special manager account that has access to all companies and has session impersonation rights. You create this account in **User Account Security Maintenance**. You activate impersonation rights on the **Options** sheet; select the **Allow System Impersonation** check box. You add companies to the user account through this program as well. For more information on User Account Security Maintenance, review the Epicor application help.

Typically this account should also be selected on the system agent in **System Agent Maintenance**. If you use a different user account on the system agent, make sure it can access all companies and sites, as this account runs processes like MRP and scheduling.

When Task Agent is configured to work with IdP, it accesses /api/.configuration endpoint for the specified AppServer URL and retrieves Identity provider URL and scope. Tokens retrieved from IdP are used for Epicor ERP as authentication.

 **Important Epicor Identity Provider** is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available **internally** to Epicor.

8. Use the **Operation Timeout** field to define how long, in seconds, it takes a server call to generate an error and fail. The default value is **86400 seconds** (24 hours).
9. If an error occurs, the task agent will try to send the call back to the server. The **Max Connection Attempts** value defines how many times the task agent will attempt to send the call again. Increase or decrease this value as you need.
10. The **Max Concurrent Tasks** field defines how many calls the task agent can send to the application server at the same time. Increase or decrease this value to reflect the capacity of your application server; the default value is **20** concurrent tasks.
11. If you use the **UsernameSslChannel** option for the Endpoint Binding type, the **Validate WCF Certificate** check box is active. This check box indicates whether the task agent service reviews the Secure Sockets Layer (SSL) Certificate to make sure this certificate is valid. When you use this option, the task agent service must be set up to run as a domain user, and this domain user account must be able to log into the Epicor application.

 **Important** If you use a self-signed certificate, do not select this check box.

12. The **DNS Endpoint Identify** field specifies the expected Domain Name System (DNS) identity of the server. If you are setting up a task agent that uses a Secure Sockets Layer (SSL) Certificate for endpoint binding, enter the identity in this field.
13. Select the **Restart Delay** value to define how long, in seconds, the Task Agent will wait before trying to restart an agent in the situation where an error has caused the agent to shut down. Possible error situations include the Application Server going offline or the system losing network connectivity. Default is 45 seconds.
14. When you finish defining the task agent properties, click **Save**.

The new task agent is created. By default, the task agent is enabled; a green icon indicates it is active.



**Important** If a task agent already exists for this application server and you attempt to save, you will receive an error. To create a new task agent for this database, you must first delete the existing task agent. After the task agent is removed, repeat the steps on this topic.



**Tip** For more information on task agents, launch the help system available in Task Agent Service Configuration.

## Windows Endpoint Configuration

You can connect a task agent to an application server through different endpoint binding types. If you will connect a new or existing task agent through the Windows endpoint binding type, you must enter a Windows domain user account on the task agent service.

The Windows domain user account you enter must be associated with either an Epicor ERP or Epicor ICE user account. Do the following to first access the Windows service and then enter the Windows domain account:

1. From the **Windows** desktop, click **Start > Control Panel**.  
The **Adjust your computer's settings** window displays.
2. Double-click on the **Administrative Tools** icon and in the next window, click the **Services** icon.  
The Services window displays.
3. Scroll through the services list until you locate the **Epicor Task Agent** icon. Right-click on this icon and select **Properties**.  
The **Epicor Task Agent Properties** window displays.
4. Click the **Log On** tab.
5. Select the **This account** radio button option.
6. Now either directly enter the **Name** for the domain user account or click the **Browse** button to find and select it. When you click the Browse button, the **Select User** window displays:
  - a. If you want to locate the domain user account by object type, click the **Object Types** button. Select the types of objects you want to include in the search and click **OK**.
  - b. Likewise click the **Locations** button to select a specific server that contains the domain user account. Select the location server and click **OK**.
  - c. Click the **Advanced** button to further limit the number of user accounts that display. Enter the filter values you need and click the **Find Now** button.
  - d. A list of domain user accounts appear. Select the domain user account you wish to use.

e. To verify the selected domain user account is valid, click the **Check Names** button.

f. If no error message appears, click **OK**.

You return to the Epicor Task Agent Properties window.



**Tip** If you receive an error message, the account is not linked to an Epicor ERP or Epicor ICE user account. Either select a different account or exit this window and create an Epicor user account. You can then repeat these steps to select the new domain user account.

**7.** Enter the **Password** for the selected domain user account.

**8.** Verify the password by entering it again in the **Confirm password** field.

**9.** Click **Apply** and then click **OK**.

You have defined a Windows domain user account for the Task Agent Service. You can now create or modify a task agent to use Windows endpoint binding.

## Activate Module Licenses

---

You use the Epicor Administration Console to manage licenses for the modules and other Epicor ERP features you have purchased.

Through the Epicor Administration Console, you can import or delete licenses and view the license properties, including basic information such as the installation name, expiration date, and data on companies, license modules, and country specific functionality included in the installation.

### Launch Epicor Administration Console

**1.** Log into your server machine.

**2.** Launch the **Epicor Administration Console**.

**3.** Use the tree view to expand and select the **Server Management > [YourServer] > [ApplicationServer]** node.

You can now expand the license node for the current application server.

### Import License File

Use this procedure to import a product license.



**Note** If the license file is already imported, this process does not generate an error or create duplicate license files. The Epicor Administration Console assumes you have run an update that contains new details from the imported license file.

**1.** In the Epicor Administration Console select the application server and then select the **Licensing** node.

**2.** Right-click the **Licensing** node and select **Import License File**.

OR

In the **Actions** menu select **Import License File**.

3. In the **Import Epicor License File** dialog box, select the license file and click **Open**.

The license file is imported and the licensed product features can be used.

## View and Edit License Properties

Use this procedure to view or edit the licensing properties of an existing installation.

1. Select the application server and the **Licensing** node.
2. Highlight the **Installation Name** for the installation you want to view or edit licensing properties.
3. Click the **Actions** menu and select **Properties**, right-click the installation and choose **Properties**, or navigate to the **Actions** pane and select **Properties**.  
The <License Name> **Properties** window displays. You can now view or edit the license properties as you need.
4. Click on the **Installation** tab to review the name of the license, when it expires, and how many users are included in the license.
5. Review the **Assigned Companies** tab to see what companies are currently included with this license.
6. Click the **Modules** tab to administrate the modules included with the license. If the module was purchased, its **Licensed** check box is selected.
7. To activate a module, select its **Enabled** check box.



**Important** Be sure you carefully review which modules you have enabled. If you do not enable modules required for your business flow, you may corrupt data. Be aware that when you enable a new module, you are committing to basic configuration and implementation steps within the Epicor ERP application. Review the Company Configuration documentation within the application help or the Epicor Implementation User Guide to learn about the primary options for each module.

8. The **Country Specific Functionality** tab displays all the localization licenses included with this license. Just like the Modules tab, if the localization is purchased, its **Licensed** check box is selected. To activate the localization, select its **Enabled** check box.



**Important** Be sure to carefully review which CSFs you have enabled. If you enable a new CSF, you must perform additional configuration steps. Review the Configure Country Specific Functionality section in the Epicor ERP Installation Guide and CSF Functionality Guides for instructions.

9. Click **OK** after you finished viewing or editing the license properties.

## License States

You use the icons that display on the License node to review the current state of each license. These icons indicate when the license is active, nearing its expiration date, or expired.

The following table describes the license states that appear on the License node.

Icon	License State
	<b>Active</b> -- This icon displays either when the license does not have an expiration date or when the license's expiration date is more than three months in the future.
	<b>Warning</b> -- This icon appears either when the license will expire today or when the license's expiration date is less than three months in the future.
	<b>Expired</b> -- This icon appears when the license is expired. Users will not be able to access the programs within this module.

## Delete License

Use this procedure to delete a license.

1. In the Epicor Administration Console select the application server, select the **Licensing** node, and then select the installation (license) that you want to delete.
2. Right-click the installation and select **Delete License**.  
OR  
In the **Actions** menu select **Delete License**.
3. In the confirmation window, click **Yes**.

## Update License

Use this procedure to update your license.

Epicor sends license updates if your company requests access to new modules. Review the Update Available column to check if any license has an update ready to be applied.

1. In the Epicor Administration Console select the application server, select the **Licensing** node, and then select the installation (license) that you want to update.
2. Right-click the installation and select **Update License**.  
OR  
In the **Actions** menu select **Update License**.
3. In the confirmation window, click **Yes**.
4. After you update the license, enable the required modules manually.

## Review Users and Licenses

---

To evaluate the system, you may need to find out how many users are active in the production environment at a specific time. You may also need to see how many licenses are available on your system.

You can check on the active users and licenses through the Epicor Administration Console. The next topics describe how you use this tool to review the active users and licenses.

### Check Active Users

To see how many users are currently logged into the application, do the following steps.

Each user is logged in as a separate session. When you display the session information for a selected application server, you can filter the information to only display the sessions currently in use.

1. Access your server machine.
2. Launch the **Epicor Administration Console**.
3. From the tree view, expand the **Server Management > [YourServerName]** node.
4. Select the application server you want to review.  
A **Connection** dialog box displays. The center pane displays the connection information for the selected application server.
5. Expand the application server node.
6. Select the **Sessions** node.  
The **Actions** pane displays a series of filter options.
7. Scroll down to the **License Usage Filter** options.
8. Clear (remove) the check next to the **Select All** option.
9. Now select the **In Use** filter option.

The center pane now only displays the users who are currently logged into the Epicor ERP application.

### Check Active Licenses

To see how many users are currently logged into the application, do the following steps.

1. Access your server machine.
2. Launch the **Epicor Administration Console**.
3. From the tree view, expand the **Server Management > [YourServerName]** node.
4. Select the application server you want to review.  
A **Connection** dialog box displays. The center pane displays the connection information for the selected application server.
5. Expand the application server node.

6. Select the **Licensing** node.  
The licenses assigned to the current application server display in the center pane.
7. Right-click a license; from the context menu, select **Properties**.  
The **[LicenseName] Properties** window displays. The **Installation** tab appears by default.
8. The **User Licenses** grid has a series of columns that display the activity of each license type. Scroll to the right to see the **Available**, **ActiveUsers**, and **MaxUsers** values.

These values indicate how many licenses are available. For example if the MaxUsers value is 20 and the ActiveUsers value is 11, then the Available column indicates 9 additional regular/full office users can log in before you run out of licenses.

## Rebuild Indexes

---

You can improve query processing for SQL Server databases by rebuilding their indexes. By rebuilding indexes through a regular schedule, you insure that Epicor ERP databases run querying tasks using optimal performance.

Each table in the Epicor ERP database is structured to contain indexes on primary key columns. When users run a query against a database, SQL Server first locates an index that contains this value and then locates the entire row of data linked to this index. This selected row is then returned to the query results. However as users add new records to the database, they fill up the free space allotted to each page within the index. This slows the response time for queries. This free space, or **fill factor**, is not actively maintained by SQL Server, so as the database expands, these indexes start to contain too much data.

To improve query performance, you need to periodically run the **Rebuild Index** task against the database. When you activate this task, you cause SQL Server to re-create the indexes on the database tables. This refreshes each index with a new fill factor, providing more free space for each page on the index. When you run this task automatically through a maintenance plan, you ensure the Epicor ERP database is regularly refreshed. It is recommended you rebuild indexes on Epicor ERP databases once each month.

## Create Index Maintenance Plan

You create a regular rebuild index maintenance plan through SQL Server Management Studio. Use the Maintenance Plan Wizard to select the Rebuild Index task and assign it to a monthly schedule.

1. On your server machine, launch **Microsoft® SQL Server Management Studio®**.
2. Right-click the **Maintenance Plans** node; from the context menu, select the **Maintenance Plan Wizard** option.  
The **Maintenance Plan Wizard** window displays.
3. Click **Next**.  
The **Select Plan Properties** window displays.
4. Enter the **Name** and **Description** you need. These values identify the maintenance plan; for example, enter IndexRebuild and for the Description, enter "Index Rebuild Plan for My Database."
5. Now select the **Single schedule for the entire plant or no schedule** radio button option. Because you will only have one task assigned to this plan, you only need one schedule for the entire plan.
6. Now next to the **Schedule** field, click the **Change...** button.

The **New Job Schedule** window displays.

7. For the **Schedule type**, verify the **Recurring** option displays.
8. Indicate you want this plan to run once a month. From the **Occurs** drop-down list, select the **Monthly** option.
9. By default, this maintenance plan will run the first day of each month. If you need change this value, use the accompanying radio button option to select a different recurring day of the week. This defines the day of the month when this maintenance plan activates.
10. Click **OK**.  
The schedule you defined now displays on the **Select Plan Properties** window.
11. Click **Next**.  
The **Select Maintenance Tasks** wizard step displays.
12. Select the **Rebuild Index** check box.
13. Click **Next**.  
The **Select Maintenance Task Order** window displays.
14. You only have one task in this maintenance plan. Click **Next**.

The **Define Rebuild Index Task** window displays.

## Define Rebuild Index Task

You next indicate how this maintenance plan will rebuild indexes.

Define the following options on the Define Rebuild Index Task window:

1. From the **Database** drop-down list, click the **Down Arrow**.  
A window displays; this window contains your available databases.
2. Select the database or databases you will rebuild.
3. Now from the **Object** drop-down list, select the **Tables and views** option. This indicates you will rebuild all the indexes in the selected database.
4. You next determine how much free space (fill factor) this plan creates from each index page. Available options:
  - **Default free space per page** - Select this option to rebuild the indexes using the fill factor defined when the indexes were originally created.
  - **Change free space per page to** - Use this option to manually enter a percentage value. While this maintenance plan runs, each index page expands using this percentage size.
5. Optionally select the **Sort results in tempdb** check box to activate the **SORT\_IN\_TEMPDB** option, which causes the plan to temporarily store intermediate search results. If a sort operation is not required or if the sort can be run in memory, the plan ignores the sort option.
6. Likewise, optionally select **Keep index online while reindexing** check box. Users can then access the table or clustered index data during index searches.

Selecting this check box activates a couple radio button options that determine how you want handle index types that do support online index rebuilds. Available options:

- a. **Do not rebuild indexes** - These indexes are ignored by the maintenance plan.
- b. **Rebuild indexes offline** - These indexes are rebuilt when they are no longer online.

**7. Click Next.**

The **Select Report Options** window displays.

## Finish the Plan

You now use the Select Report Options indicate how you want the system to notify you when the maintenance plan runs.

1. Select the **Write a report to a text file** check box to write a .txt file to a specific directory. Click the **Browse** (...) button to find and select this directory.
2. Select the **E-mail Report** check box to activate the **To:** operators list. Select the individual who will receive this e-mail report from this drop-down list.
3. **Click Next.**  
The **Complete the Wizard** window displays.
4. Review the maintenance plan options you selected. Click the **Back** button to makes any changes you need.
5. **Click Finish.**

The Rebuild Index maintenance plan is now active. Each time the system clock activates the day of the month you selected, the indexes are automatically rebuilt on the selected database(s).

## Regenerate Data Model

---

Users can customize their Epicor application database by adding either user-defined (UD) table and column extensions to existing tables or new tables and columns.

You can add user-defined (UD) columns to existing tables through the **UD Columns Maintenance** program. Additionally, new tables and columns can be added through the Software Developers Kit (SDK) for company specific data extensions.



**Important** Regenerating the data model must be completed to incorporate the new and extended tables and columns. You can run data model regeneration from the Epicor Administration Console. When you regenerate the data model in the Epicor Administration Console, the application saves the tracing log in the **temp%\Epicor\** folder. You can also launch this process through a command line prompt, a desktop icon, or a recurring system task. Set up these launch options when you frequently regenerate the data model, as these methods provide a faster way to activate this process.

You can also extend your Epicor application database with new tables through the Software Developers Kit (SDK). Extensions to ERP possess their own data models, which are stored alongside the main ERP data model. Data Model Generator command line tool creates a data model for the new extension. To do this, the configuration file needs to be modified (see [Example Configuration Files](#)).

## Epicor Administration Console Option

If you occasionally need to regenerate the data model, run this process through Epicor Administration Console. The regeneration process is set up to update the current database selected on the tree view.

### Launch from Console

Do the following to launch the data model regeneration process from the Epicor Administration Console.

1. On your server machine, press **<Windows> + F** to display the **Search** bar.
2. Use one of these options to launch your search:
  - a. From the **Search** drop-down list, select the **Everywhere** option. In the search field, enter **Epicor Administration Console**.
  - b. Click on the **Apps** button.  
The Apps screen displays.
3. Locate the **Epicor Software** section on this screen and click the **Epicor Administration Console** icon.
4. From the tree view, expand the **Database Server Management** node and the node for the database server that contains the database you wish to regenerate.
5. Select the database.  
The properties for the database displays in the center pane.
6. From either the **Action** menu or the **Actions** pane, select **Regenerate Data Model**.  
The **Generate Data Model** dialog box opens.
7. Adjust or verify the settings in the dialog box:
  - **Server name** - SQL Server **server\Instance** name where the database is located. Initially populated with the database server for the selected database.
  - **Database name** - The database for which you are regenerating the database model. Initially populated with the selected database.
  - **Authentication** - If you select Windows Authentication, the **User name** and **Password** default to your current login values. If you select SQL Server Authentication, enter the user account and password you use to log into SQL Server.
8. Click **Generate**.



**Important** If you receive an error that the .dll file for the data model generation is in use by another process, end the task. Launch the Internet Information Services Manager by clicking **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**. Select the **Application Pools** node; the center pane displays the application pools available on your system. Right-click your application server node; from the context menu, select **Recycle**. You should be able to regenerate the data model.

Likewise if you receive an error that states some tables did not synchronize, you can review the log file to see more details about these table errors. The location of this log file displays in the error message.

When you successfully regenerate the data model, a dialog box displays. Click **OK**.

9. Now to complete this process, you must pull the latest data model from the database and copy it to the local application server by recycling the application pool. Recycling the application pool is a mandatory task after the data model successfully regenerates. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
  10. Expand the tree view and select the **Application Pools** node.  
The center pane displays the application pools available on your system.
  11. Right-click on the application pool for your application server; from the context menu, select **Recycle**.
-  **Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The regenerate process stages the data model in the database. When the application server restarts, the Epicor ERP application checks the data model on both the disk and the database. If a new data model version is available, this version is retrieved from staging and the database is updated to include the user-defined table. Epicor users can now view and enter data in the user-defined columns.

 **Important** When you reference these user-defined columns through either programming or a customization, the columns appear to be part of the base (primary) table because the data model merges the two tables into one logical entity. To identify the UD columns, their identifiers all use the ".c" suffix.

If you need to regenerate the data model more often, consider running this process through a command line, a desktop icon, or a recurring task. These launch options are explained in the Epicor Administration Console help, Command Line Tools Guide and the System Administration Guide.

## Standalone Launch Options

You can also configure the data model regeneration process to run through a standalone launch option. Use these options when you frequently need to regenerate the data model.

You can launch data model regeneration through these standalone options:

- **Command-Line** - Run this process by executing it from either the **Command** or **Powershell** windows.
- **Desktop Icon** - Create a shortcut icon for the data model regeneration process. You can then launch this process from your desktop.
- **Recurring System Task** - Add this process as a system task and assign it to a schedule. When the system clock activates this schedule, the data model regenerates.

## Modify the Data Model Generator File

You first define the overall settings for the regeneration process. You modify these settings in the DataModelGenerator.exe.config file.

To modify this file:

1. Navigate to the **DataModelGenerator** folder on your client installation. For example:  
C:\Epicor\[YourEpicorEnvironment]\DataModelGenerator
2. Open the **DataModelGenerator.exe.config** file in **Notepad** or a similar text editor.

3. Modify the **GenerateAll** setting to indicate whether you want to generate all the data models in this environment or only the data model that matches the current system code. Typically you want to generate all the data models; if this is the case, enter "true" for this setting.
4. Likewise modify the **StoreInDB** setting to indicate whether you want the data model assembly to be stored in the database. You also typically enter "true" for this setting.
5. Save the **DataModelGenerator.exe.config** file.

## Modify the Configuration File

You next modify your client .sysconfig file so the data model regeneration process updates a specific database within your Epicor environment.

1. Navigate to the **config** folder on your client installation. For example:  
C:\Epicor\[YourEpicorEnvironment]\Client\Config
2. Open your **.sysconfig** file (such as MySettings.sysconfig) in **NotePad** or a similar text editor.
3. Configure your .sysconfig file so it updates your database.

For example:

```
<configuration>
  <toolsSettings>
    <TargetLocation value="C:\Users\MyUser\AppData\Local\Temp\Epicor\DataMode
lGenerator" />
    <SystemCode value="ERP" />
    <DBServer value="(local)" />
    <DBName value="ERP10Staging" />
    <IntegratedSecurity value="true" />
    <UserID value="" />
    <Password value="" />
  </toolsSettings>
</configuration>
```

4. **Save** the .sysconfig file.

You can now specify this .sysconfig file when you run the data model regeneration process. You do this on the command line, the **Target** field for a desktop icon, or in the arguments for a recurring system task. The following sections include information on how to set up each launch option to use your modified .sysconfig file.

## Launch from Command Line

You can run the data model regeneration process directly from the command line in your Command or PowerShell window.

To start the process from the command line:

1. Launch either the **Command** or **PowerShell** windows.
2. At the **C:\** prompt, change directories to the client location of the **Data Model Generator**. For example:  
**C:\Program Files (x86)\Common Files\Epicor Software\Database Manager Extensions\[ICE Version]\DataModelGenerator**
3. Enter the **Ice.Tool.DataModelGenerator.CL.exe** command.

4. Optionally specify that the data model regeneration process will use your configuration settings file. Enter **-config** followed by the .sysconfig file directory and name in quotes. For example: **-config="C:\Epicor\[YourEpicorEnvironment]\Client\Config\MySettings.sysconfig"**



**Tip** If you do not specify a .sysconfig file, the regeneration process uses the default .sysconfig file for this client installation.

5. Press **[Enter]**.

The data model regeneration process runs against the database specified in the .sysconfig file. It refreshes the structure of the tables in the database.

6. Now to complete this process, you must pull the latest data model from the database and copy it to the local application server by recycling the application pool. Recycling the application pool is a mandatory task after the data model successfully regenerates. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

7. Select the **Application Pools** node.

The center pane displays the application pools available on your system.

8. Right-click on the application pool for your application server; from the context menu, select **Recycle**.



**Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The regenerate process stages the data model in the database. When the application server restarts, the Epicor ERP application checks the data model on both the disk and the database. If a new data model version is available, this version is retrieved from staging and the database is updated to include the user-defined table. Epicor users can now view and enter data in the user-defined columns.



**Important** When you reference these user-defined columns through either programming or a customization, the columns appear to be part of the base (primary) table because the data model merges the two tables into one logical entity. To identify the custom columns, their identifiers all use the "\_c" suffix.

## Launch from Desktop Icon

You can also run the data model regeneration process from a desktop shortcut icon. Like the command line option, you can run the data model regeneration using a specific .sysconfig file.

1. On your server machine, navigate to the **DataModelGenerator** folder. For example: **C:\Epicor\[YourEpicorEnvironment]\DataModelGenerator**
2. Locate the **DataModelGenerator.exe** icon.
3. Right-click this icon; from the context menu, select **Create shortcut**. The **Data Model Generator** icon displays on your desktop.
4. Optionally, specify the data model regeneration process runs using a specific configuration settings file. Right click the desktop icon; from the context menu, select **Properties**. The **Properties** window displays.
5. In the **Target** field add a **-config** runtime argument followed by the .sysconfig file directory and name in quotes. For example: **-config=" C:\Epicor\[YourEpicorEnvironment]\Client\Config\MySettings.sysconfig"**



**Tip** If you do not specify a .sysconfig file, the regeneration process uses the default .sysconfig file for this client installation.

**6.** Click **Apply** and then **OK**.

When you click this desktop icon, the data model regeneration process runs against the database specified in the .sysconfig file. It refreshes the structure of the tables in the database.

Now to complete this process, you must pull the latest data model from the database and copy it to the local application server by recycling the application pool. Recycling the application pool is a mandatory task after the data model successfully regenerates. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**. Select the **Application Pools** node. The center pane displays the application pools available on your system. Right-click on the application pool for your application server; from the context menu, select **Recycle**.



**Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The regenerate process stages the data model in the database. When the application server restarts, the Epicor ERP application checks the data model on both the disk and the database. If a new data model version is available, this version is retrieved from staging and the database is updated to include the user-defined table. Epicor users can now view and enter data in the user-defined columns.



**Important** When you reference these user defined columns through either programming or a customization, the columns appear to be part of the base (primary) table because the data model merges the two tables into one logical entity. To identify the custom columns, their identifiers all use the "\_c" suffix.

## Launch as a Recurring Task

If you need to regularly regenerate the data model, set up this process to run through a recurring system task. Because this process runs through a command line .exe, you can set it up as a task within Windows® Task Scheduler® or a similar task scheduling application.

The following instructions describe how you set up data model regeneration as a regular task through Windows Task Scheduler. You follow similar steps in other task applications.

- 1.** Access your **Control Panel** and click the **Administrative Tools** icon.  
The **Administrative Tools** window displays.
- 2.** Select the **Task Scheduler** icon.  
The **Task Scheduler** window launches.
- 3.** Click **Action > Create Basic Task**.  
The **Create Basic Task** wizard displays.
- 4.** Enter a **Name** for the task. For example: Data Model Regen - Daily
- 5.** Now enter a concise **Description** for the task. For example: "This task runs the data model regeneration process each night."
- 6.** Click **Next**.
- 7.** For the **When do you want the task to start?** wizard step, select how often you want the task to run. For this recurring example, select the **Daily** radio button option.

8. Click **Next**.
9. Now indicate the **Start Date** when you want this recurring task to begin.
10. In the **Recur** field option, define how often you want this task to run. For this example, you select **Recur every 1 days**.
11. Click **Next**.
12. For the **What action do you want the task to perform?** wizard step, select the **Start a program** radio button option.
13. Click **Next**.
14. Now click the **Browse...** button to find and select the **DataModelGenerator.exe** file on your client installation. For example: **C:\Epicor\[YourEpicorEnvironment]\DataModelGenerator**
15. Lastly in the **Add arguments (optional)** field, you can add a –config runtime argument followed by the .sysconfig file name in quotes. For example: **-config="C:\Epicor\[YourEpicorEnvironment]\Client\Config\MySettings.sysconfig"**
16. Click **Next**.
17. Review the options you selected. If you need to make changes, click the **<Back** button. When you are satisfied with the task, click **Finish**.

When the system clock activates the recurring schedule you defined, the data model regenerates, updating the structure of the selected database.

Now to complete this process, you must pull the latest data model from the database and copy it to the local application server by recycling the application pool. Recycling the application pool is a mandatory task after the data model successfully regenerates. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**. Select the **Application Pools** node. The center pane displays the application pools available on your system. Right-click on the application pool for your application server; from the context menu, select **Recycle**.

 **Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The regenerate process stages the data model in the database. When the application server restarts, the Epicor ERP application checks the data model on both the disk and the database. If a new data model version is available, this version is retrieved from staging and the database is updated to include the user-defined table. Epicor users can now view and enter data in the user-defined columns.

 **Important** When you reference these user defined columns through either programming or a customization, the columns appear to be part of the base (primary) table because the data model merges the two tables into one logical entity. To identify the custom columns, their identifiers all use the "\_c" suffix.

## Data Model Customization

This section describes how you can customize what tables update through the data model regeneration process. By leveraging these features, you can configure the process to update the specific tables and schemas you need.

### Table Standards

If you are adding a custom table to the database, it must match the database requirements for the Epicor ERP application. The custom table will then be included when the data model regenerates.

Before you regenerate the data model, be sure your custom table follows these standards. Each custom table must have:

- A primary key.
- A SysRowID column with NOT NULL as its unique identifier.
- Table and column names that only have letters, numbers, and underscore characters.



**Important** Any tables that do not follow these standards are removed from the list of included tables and so are ignored by the data model regeneration process. Users cannot select these tables on customizations or Business Process Management (BPM) directives.

### Included and Excluded Tables

The following tables are either included or excluded in the regenerate data model process.

Included tables:

- All tables in Epicor ERP shipped schemas; typically these tables use the **Ice** and **Erp** prefixes.
- Table schemas specified through the **IncludeSchemas** configuration setting. If you wish to include custom tables, you need to add them using this configuration setting. The following Include Schemas topic describes how you update this setting with custom schemas.

Excluded tables:

- Tables listed in the **ExcludeTables** configuration setting. If you wish to exclude tables, you need to add them using this configuration setting. The following Exclude Tables topic describes how you add tables to this custom setting.
- Tables that use the **cdc**, **IM**, and **dbo** prefixes are never included in the data model.

### Include Schemas

To include your custom tables from other schemas, modify the **IncludeSchemas** setting by adding your custom prefix values to it. The next time you regenerate the database, your custom tables are included in the data model.

For example, you have created a series of "Prod" and "Fin" custom tables to handle unique production and financial data required by the products you manufacture. To update the configuration file:

1. Navigate to the Data Model Generator directory; typically this will be the **C:\Epicor\[YourEpicorEnvironment]\DataModelGenerator** directory path.
2. Now modify the .config file for the option you use to launch the data model regeneration process:
  - If you run this process through the Epicor Administration Console, locate the **Ice.Tool.DataModelGenerator.Ui.exe.config** file, typically found in **C:\Program Files (x86)\Common Files\Epicor Software\Database Manager Extensions\[ICE Version]\DataModelGenerator**.

- If you run this process from a command line, desktop icon, or recurring system task, locate the **DataModelGenerator.exe.config** file, typically found in C:\Epicor\[YourEpicorEnvironment]\DataModelGenerator.

3. Open either .config file in **Notepad** or a similar text editor.
4. Locate the **IncludeSchemas** setting.
5. Add the custom table prefixes as a value list inside this setting. For example:

```
<setting name="IncludeSchemas" serializeAs="String">
    <value>Prod,Fin</value>
</setting>
```

6. **Save** the configuration file.
7. **Close** the text editor.

Now the next time you regenerate the data model, these custom schemas are included in the data model regeneration process.

## Exclude Tables

You can also use the configuration files to exclude specific tables from the data model. When you run the data model regeneration process, these tables are ignored and so are not added to the data model.

1. Navigate to the Data Model Generator directory; typically this will be the **C:\Epicor\[YourEpicorEnvironment]\DataModelGenerator** directory path.
2. Now modify the .config file for the option you use to launch the data model regeneration process:
  - If you run this process through the Epicor Administration Console, locate the **Ice.Tool.DataModelGenerator.Ui.exe.config** file.
  - If you run this process from a command line, desktop icon, or recurring system task, locate the **DataModelGenerator.exe.config** file.
3. Open either .config file in **Notepad** or a similar text editor.
4. Locate the **ExcludeTables** setting.
5. Enter the specific tables you wish to exclude from the data model. Separate each table with a comma. For example:

```
<setting name="ExcludeTables" serializeAs="String">
    <value>Ice.SysSequence,Ice.DBMigrationLog,Ice.SessionState,Ice.SysAgentSchedProcessing</value>
</setting>
```
6. **Save** the configuration file.
7. **Close** the text editor.

The next time you regenerate the data model, the regeneration process ignores the listed tables.

## Manual Database Backup

A frequent task you will do is create a manual backup of the entire database. This full backup is then available for various purposes such as archiving databases, creating a new test environment, saving a database offsite, and so on.

You can manually backup a database whenever you need. You typically create a manual, "on-the-fly" backup when you want to make a complete copy without having to shut off the database. You can then store this separate, independent copy in a different location.

### Run the Backup

The following steps illustrates how you create a manual backup of the entire database.

1. Launch **Microsoft® SQL Server Management Studio®** and connect to your server.
2. Within the **Object Explorer**, right-click the database you want to back up, and select the **Tasks > Backup...** option.  
The **Back Up Database** window displays.
3. From the **Database** drop-down list, select the database you want to backup.
4. For the **Backup type**, select the **Full** option. You should always select this option for an "on-the-fly" backup, as all the data will then be recorded in this backup file.
5. Now select the **Copy-only Backup** option. This indicates you are making a separate copy of the database independent from your scheduled, recurring back-ups (Recurring backups are explored in the next section). You should always select this check box when running a manual, "on-the-fly" backup.



**Important** Recurring full and transaction log backups create a backup chain where each backup builds off the previous backup. If you run a manual or "on-the-fly" backup and do not select this check box, you will interrupt this backup chain. All transactional log backups can only build from this "on-the-fly" full backup, and so you will not be able to restore from any transaction log backups made before this backup.

6. You next identify the **Destination** where the backup database copy will be stored. Notice you can save the backup to either a directory location or a device (if a device is installed). With the **Disk** radio button option selected, click the **Add** button.

The **Select Backup Destination** window displays.

7. Click the **Browse...** button to find and select the directory path. For example, navigate to the C:\Epicor\ERP10\ERP10.00.600 path.
8. You also enter the **Filename** used for the backup. For example, enter <DatabaseName>Full.



**Tip** For the backup file name, use the same name as the database. This convention helps keep the backup files organized.

9. Click **OK** to close the browse window and **OK** again to close the **Select Backup Destination** window. You return to the Back Up Database window.

10. Notice the default destination still displays, so you could back up this database in two locations. You only need one backup. Highlight the default option that backs up the file to Microsoft SQL Server; click **Remove**.
11. From the tree view, select the **Backup Options** node.
12. Enter the **Name** for the backup. This value is important, as it will help you quickly locate the backup file later when you need to restore the database. You should shorten the name to <DatabaseName>FullManual or something similar.
13. Use the **Description** field to enter more information you need about the backup.
14. You can also indicate when you wish to discard the backup using the **Backup set will expire** options. These options are helpful for removing older backups to free up space on your backup disk.
  - **After** - Defines a period of days that pass before the backup database is removed. Use the accompanying field to define the number of days.
  - **On** - Specifies a specific date on which the database expires. When you select this option, you define a specific date on which this backup will expire.
15. From the **Set backup compression** drop-down list, select the **Compress backup** option.  
By compressing the backup, you improve performance. The backups also take less space on your disk.
16. From the tree view, select the **Media Options** node.
17. In the **Overwrite Media** pane, verify the **Back up to the existing media set** radio button option is selected.
18. Now select the **Overwrite all existing backup sets** radio button option. This reduces the number of backup datasets in the backup disk location.
19. Click **OK**.  
Watch the progress bar to check on the backup.
20. When finished, a message displays, indicating the backup was successful. Click **OK**.  
The manual backup is now complete.
21. To see the file, navigate to the folder you selected for the backup location.

The database backup file displays.

## Backup Maintenance Plan

---

You need to define a back up plan to ensure a recent snapshot of your organization's current data is available. When an emergency happens, you can then restore the database from a recent backup and significantly reduce how much data is lost.

Before you begin, plan your backup strategy. Consider both your **Recovery Time Objective** (RTO) and your **Recovery Point Objective** (RPO). RTO defines how long your organization is willing to wait for the data to restore after a failure. Since the database cannot be updated during the recovery process, deciding how long the recovery can take affects what backup types you select and schedule. RPO defines how much data you are willing to lose after a failure; for example, is your organization able to recover data from a 5:00 pm full backup, or is a more recent 5:30 differential backup and a 5:45 transaction log backup required? Once you determine these recovery objectives, you can develop the backup plan that works the best for your organization.

Through Microsoft® SQL Server Management Studio®, you can back up data manually (on-the-fly) or through a regular, recurring schedule. Work with the managers at your organization to determine how often each database should be backed up, and the most ideal times to run the backups. You may need to take backup copies off site for extra security in the event of a disaster. Do not put yourself in a position where you cannot restore most of your organization's data.

Things to consider as you develop the backup strategy for each database:

- **How important is the data?** If the data is crucial to an area of your business, you should back it up often, preferably through a regular schedule.
- **Does the data change frequently?** The more the data changes, the more backups you should run against the database. This ensures most of the recent data is not lost.
- **How fast do you need to restore the data?** If you need to recover the data quickly to resume business operations, you should run full backups. By restoring from a full backup, all the data is restored immediately. If the data does not need to be restored right away, consider adding differential and transactional log backups in your plan. Restoring data through these recovery types takes longer, as you need to restore each transactional log backup in date/time sequence from the most recent differential backup. However you will likely lose less data.
- **Do you have adequate equipment to run and store the backup databases?** Review the backup needs with managers to make sure your system hardware can handle running and storing the backups.
- **What is the best time to schedule backups?** Locate an after hours period in the schedule when less users access the database.
- **What is your plan for storing the backups off-site?** Develop a regular system where each database is moved off site. In case of a major emergency, this backup data is secure.



**Tip** While you must back up your Epicor data, you do not need to back up the SSRS report server the Epicor ERP application creates. You connect application servers to the SSRS server, so the SSRS report server contains data that already exists in your Epicor databases.

## Create Maintenance Plan

1. Within the Object Explorer, expand the **Management** node.
2. Right-click the **Maintenance Plans** node; from the context menu, select the **Maintenance Plan Wizard** option.

The **Maintenance Plan Wizard** window displays.

3. Click **Next**.

The **Select Plan Properties** window displays.

4. Enter the **Name** and **Description** you need. These values identify the maintenance plan; for example, enter DBBackupPlan and for the Description, enter "Backup Maintenance Plan for My Database."

5. Now select the **Separate schedules for each task** radio button option. This indicates each task you activate on this maintenance plan will have a unique, recurring schedule.

6. Click **Next**.

The **Select Maintenance Tasks** wizard step displays.

7. Select the following tasks:

- **Check Database Integrity**
- **Back Up Database (Full)**

- **Back Up Database (Differential)**
- **Back Up Database (Transaction Log)**

**8.** Click **Next**.

The **Select Maintenance Task Order** wizard step displays.

**9.** Because you indicated each task will run through a different schedule, you do not need to change the order in which these tasks are run. Click **Next**.

You now set up the database check integrity task.

## Check Database Integrity

You need to frequently validate the allocation and structural integrity of user and system tables by running the DBCC CHECKDB Transact-SQL statement. Running this task ensures any database integrity problems are reported.

You should now see the **Define Database Check Integrity Task** wizard step.

- 1.** Click the **Databases** drop-down list.
- 2.** From the radio button options, select the **These databases** option.
- 3.** Select the **<DatabaseName>** check box.
- 4.** Click **OK**.
- 5.** Now define the specific schedule the database integrity task will use. Click the **Change...** button.

The **New Job Schedule** window displays.

Use the options on this window to define how often you want this automatic schedule to run. Be sure you select a date/time when database activity is low.

- 6.** From the **Schedule type** drop-down list, select the **Recurring** option. This schedule then activates automatically. Verify the **Enabled** check box is selected.
- 7.** Now define how often this task will run. Typically you check for database integrity once a week, although you can run this task more often if your system has enough resources. For example, you can click the **Occurs** drop-down list and select **Weekly**.
- 8.** For the **Recurs every** value, enter a numeric value in this field, then select a day of the week option. For example, if you select the Sunday day option, this task runs every Sunday.
- 9.** Now select the **No end date** radio button option to insure this task continuously runs.
- 10.** Review the options you selected in the **Description** field. If you are satisfied with this job schedule, click **OK**.
- 11.** You are ready to set up another task. Click **Next**.

## Define Full Backup

Now use the **Define Back Up Database (Full) Task** window to set up the database backup task.

1. Click the **Database(s)** field. From the database options, select the **[DatabaseName]** checkbox and click **OK**.  
The Database(s) field now displays the **Specific databases** value.
2. For the **Backup** component, verify **Database** is selected.
3. For the **Back up to:** option, select **Disk**.
4. Click the **Destination** tab.
5. Verify the **Create a backup file for every database** radio button option is selected.
6. Notice the **Folder:** field; you can click the **Browse (...)** button next to this field to pick a different directory for the backup file.
7. Click the **Options** tab.
8. From the **Set backup compression** drop-down list, select the **Compress backup** option.  
By compressing the backup, you improve performance. The backups also take less space on your disk.
9. Now indicate how long this backup will be available. Select the **Backup set will expire:** check box and then select the **After** radio button option. Enter a value you need; the default value is 14 days.
10. Select the **Verify backup integrity** check box. Selecting this check box ensures the database contains valid data you can successfully recover.
11. Now create the schedule for this full database backup task. Click the **Change...** button.  
The **New Job Schedule** window displays.
12. You want this full backup to run every day. To do this, enter the following values:
  - a. **Schedule type:** Select the Recurring option and the Enabled check box.
  - b. **Frequency:** Select the Daily option.
  - c. **Daily Frequency:** Accept the Occurs once at: 12:00:00 AM value. This value assumes there is less database activity during this time; if a different time is better for your organization, change this time.
  - d. **Duration:** If you select the No end date radio button option, this task continuously runs.
13. When you finish setting up these schedule options, click **OK**.
14. Now you'll set up the Differential task. Click **Next**.

## Define Differential Backup

Differential database backups save the database changes that occurred since the previous full backup. You should run this backup type through an hourly schedule; you then first recover from the most recent full backup and then the most recent differential backup.

1. Click the **Database(s)** field. From the database options, select the **[YourDatabaseName]** checkbox and click **OK**.
2. For the **Backup component**, verify **[YourDatabaseName]** is selected.
3. For the **Back up to:** option, select **Disk**.
4. Now click on the **Destination** tab.
5. Verify the **Create a backup file for every database** radio button option is selected.
6. Now click on the **Options** tab.
7. From the **Set backup compression** drop-down list, select the **Compress backup** option.
8. Now indicate how long this backup will be available. Select the **Backup set will expire**: check box and then select the **After** radio button option. Enter a value you need; the default value is 14 days.
9. Now create the schedule for this differential database backup task. Click the **Change...** button. The **New Job Schedule** window displays.
10. You need the differential task to run once each day. To do this, enter the following values:
  - a. **Schedule type:** Select the Recurring option and the Enabled check box.
  - b. **Frequency:** Select the Daily option.
  - c. **Daily Frequency:** Select the Occurs every: 1 hour(s) value. This means the transaction log backup will run once each hour throughout the day.
  - d. **Duration:** If you select the No end date radio button option, this task continuously runs.
11. When you finish setting up these schedule options, click **OK**.
12. Now you'll set up the Transaction Log backup task. Click **Next**.

## Define Transaction Log Backup

Transaction Log database backups are saved outside the full and differential backups. You use this backup to restore all the transactions that occur after the most recent differential backup.

After you determine the differential backup you will use, you then restore each subsequent transaction log backup in date/time order. Each backup then builds on the data saved in the previous transaction log backup.

1. Click the **Database(s)** field. From the database options, select the **[YourDatabaseName]** checkbox and click **OK**.
2. For the **Backup component**, verify **Database** is selected.

3. For the **Back up to:** option, select **Disk**.
4. Now click on the **Destination** tab.
5. Verify the **Create a backup file for every database** radio button option is selected.
6. Now click on the **Options** tab.
7. From the **Set backup compression** drop-down list, select the **Compress backup** option.
8. Now indicate how long this backup will be available. Select the **Backup set will expire**: check box and then select the **After** radio button option. Enter a value you need; the default value is 14 days.
9. Now create the schedule for this differential database backup task. Click the **Change...** button. The **New Job Schedule** window displays.
10. You need the differential task to run once each day. To do this, enter the following values:
  - a. **Schedule type:** Select the Recurring option and the Enabled check box.
  - b. **Frequency:** Select the Daily option.
  - c. **Daily Frequency:** Select the Occurs every: 10 minute(s) value. This means the transaction log backup will run every ten minutes.
  - d. **Duration:** If you select the No end date radio button option, this task continuously runs.
11. When you finish setting up these schedule options, click **OK**.  
You have set up a backup that will run every ten minutes. Now if you need to restore the database, your organization will only lose ten minutes or less of recent data.
12. Now you'll finish the maintenance plan. Click **Next**.

## Finish the Maintenance Plan

1. Use the **Select Report Options** wizard step to generate either a text file report or an email report. For this workshop, select the **Write a report to a text file** check box. Notice you can define the specific text file that will update with the back up report information.
2. Click **Next**.  
The **Complete the Wizard** window displays.
3. Expand the nodes to review your maintenance plan selections. If you wish to change an option, click the **<Back** button to modify the plan. If you are satisfied with the maintenance plan, click **Finish**.  
A window now displays that show the progress of the maintenance plan. A green **Success** check mark displays next to actions that completed. If the wizard encountered a problem, either an **Error** or a **Warning** check mark would display along with a message describing the problem.
4. Click **Close**.

The maintenance plan is now active. When the system clock on the server matches the date/time defined on a schedule for one of the maintenance plan tasks, the task runs and a backup file is created in the folder location you specified.

## Email Notification

Now that you've created the maintenance plan, you can optionally set up an email alert that notifies you when the backup fails.

To use this functionality, you must first set up SQL Server to send email notifications. You use the **Database Mail Configuration Wizard** to activate database mail. If you haven't already set this up, review this SQL Server documentation to activate this feature:

- <https://msdn.microsoft.com/en-us/library/Hh245116.aspx>

Once email notifications are active, do the following:

1. From the **Object Explorer**, expand the **SQL Server Agent** node.
2. Expand the **Jobs** node to display each job you created through your maintenance plan.
3. Right-click the full backup task (ERPDemoPlan.Subplan2); from the context menu, select **Properties**. The **Job Properties** window displays.
4. From the **Select a page** pane, select **Notifications**.
5. Click the **E-mail** check box.
6. From the first drop-down list, select the email address that will receive the notification.
7. Now from the second drop-down list, select the **When the job fails** option.
8. Click **OK**.

## Restore Database

---

If there is an emergency, you can restore the database using a back up file.

### Restore from Backup

To restore a database from a backup file:

1. On your server machine, launch the **Epicor Administration Console**.
2. Expand the **Server Management** node and select the application server for the database you need to restore.
3. From the **Actions** pane, select the **Stop Application Pool** option.
4. Navigate to the **SQL Server Management Studio**.
5. Right-click the database for which you want to restore the backup, and select the **Tasks > Restore > Database...** option.

The **Restore Database - [YourDatabaseName]** window displays.

6. From the tree view, select the **General** node.
7. Select the **Database** radio button option.  
Notice the **Backup sets to restore** grid displays the path to the manual database backup file you created.
8. Select the **Restore** check box next to the backup name you want to restore.
9. Now on the tree view, highlight the **Options** node.
10. Select the **Overwrite the existing database (WITH REPLACE)** check box.
11. From the **Recovery State** drop-down list, select the **RESTORE WITH RECOVERY** option.  
Be sure you select this option. Running the restore in this state causes the database to completely refresh with the data saved in the backup file. The other options restore through different stages; review the SQL Books documentation for more information on these features.
12. Now from the tree view, click on the **Files** node.
13. Review the directory paths to make sure you will restore the correct database.
14. Click **OK**.  
The database is restored using your selected options.
15. Return to the **Epicor Administration Console**.
16. Verify the application server you stopped is selected.
17. From the **Actions** pane, select **Start Application Pool**.

The database is restored using the selected backup file.

## Purge Database

---

You should periodically run the Database Purge and Summarize process to remove old information from the Epicor ERP application database. Removing old data makes it easier for users to locate current records and also saves space in the database file.

To determine how often you should run the database purge, consult with managers throughout your organization. Once you decide how much data can be periodically removed, set up a regular schedule to run the Database Purge and Summarize process. For example, you might decide to purge data at the end of each quarter.

This process deletes records using a Cut Off Date you enter. You also determine what categories of records to remove such as jobs, purchase orders, and/or journal entries. When you run the purge process, any records in the selected categories created on or before the Cut Off Date are permanently removed from the database.



**Important** Once you purge the database, the selected information cannot be recovered. Be sure to backup your database to another location before you run this process. Perform this procedure only if you are absolutely certain you no longer need data entered up to the Cut Off Date.

## Run the Purge

Follow these steps to permanently remove selected records from the database.

1. Navigate to the **Database Purge and Summarize** program.

**Menu Path:** System Management > Purge/Cleanup Routines > Database Purge and Summarize

2. The **Last Purged** section at the bottom of this window displays information about the previous time the database was purged. Use this information to determine if enough time has passed for you to run the database purge again.
3. Enter the **Cut Off Date** you want the purge process session to use. This value determines the last date from which records are removed from the database.  
Any selected records entered on or before this date are deleted from the database.
4. Use the rest of the check box options to determine which categories of records will be removed through the purge process. Available categories:

- a. Select the **Transactions (PartTran)** check box to remove part transaction records.

- b. If you wish to remove time and expense entries, select the **Labor** check box.

- c. Select the **Job** check box to remove jobs created on or before the Cut Off Date.

- d. Select the **Configuration Inputs** check box to remove **PcInValue** (Saved Input Values) records.



**Important** To delete a configuration input, the related source sales order, job, quote, or purchase order record must also be included in the purge process.

- e. To remove journal entries from the database select the **Journal Details** check box.

- f. Selecting this check box activates the **Summarization Journal** drop-down list. Use this list to define the journal that summarizes the purged financial records. This purge process will total the debit/credit amounts for each period from a scope of accounts, and then posts these results to the selected journal.



**Tip** To make the summarization tracking process easier, you should use a corresponding Journal Code.

- g. Select the **Purchase Order** check box to delete purchase orders created on or before the Cut Off Date.

- h. To remove old sales order forecasts and demand contract entries, select the **Demand** check box.

- i. Select the **Quote** check box to remove sales orders generated on or before the Cut Off Date.

- j. You select the **Web Basket** check box to remove any web basket product configurations created on or before the Cut Off Date.

- k. To remove **Review Journal** entries, select this check box.

The purge process will attempt to cancel any existing review journals. If the purge process cannot cancel these records, the Review Journal tables are still cleared.

- l. Select the **Change Log** check box to delete change log entries entered on or before the Cut Off Date are removed from records throughout the database.

- m. If you want to remove older sales orders, select the **Order** check box.

5. When you are ready to purge the data, click **Submit**.

Records from the selected categories created on or before the Cut Off Date are removed from the database. Now that the older records are removed, users have less old data to navigate as they search for database files.

## Purge Tasks

---

You can use **System Agent Maintenance** to purge tasks from the task agent through an automatic, regular schedule. You then no longer need to manually purge these tasks from the system.

This feature is available in **System Agent Maintenance** under the **Actions** menu. Use the **Set Purge Frequency** action to specify a task purge date range and a frequency for report purge actions.

**Menu Path:** System Setup > System Maintenance > System Agent



**Important** This program is not available in Epicor Web Access.

### Changing Task Agent Purge Settings

Do the following to change the purge settings:

1. Click the **Actions** menu and select **Set Purge Frequency**.  
The **TaskAgent Purge Frequency** window displays.
2. The **Task Purge Date Range in Days** specifies the number of days back from the current date than tasks are retained. Anything older is deleted. Enter the value you need; the default is 30 days.
3. Now enter the **Report Purge Frequency in Seconds** value. This value specifies the interval, in seconds, between report purge actions. The default is 900 seconds.

The value in this field controls only triggering of the report purge action. The exact date and time that a report is purged is determined by the date and time that the report is generated, the archive period (in days) specified in the report's configuration, and finally by the report purge frequency setting. For example:

- A report is generated on 6/17/2017 at 10:22, the Report Archive Period on the report's Summary sheet is 4 days, and Report Purge Frequency in the task agent setup is 1800 seconds.
- The report will be purged four days later on 6/21/2017 at 10:30. With the purge frequency set to 1800 seconds (on the half hour), the purge at 10:00 will ignore the report because the purge date is in the future, and the purge at 10:30 will remove it.



**Note** A Task cannot be deleted until all of its associated reports reach their purge date.

4. Click the Restore to Default button to return the purge values to the installed settings.
5. Click **OK** to use the revised purge settings.
6. Restart the task agent to activate the revised purge settings:
  - a. On the server machine, open the All Programs > Epicor Software > Epicor Administrative Tools > Epicor ICE Task Agent Service > TaskAgent Service Configuration .
  - b. From the **Actions** menu, select **Restart Service**.

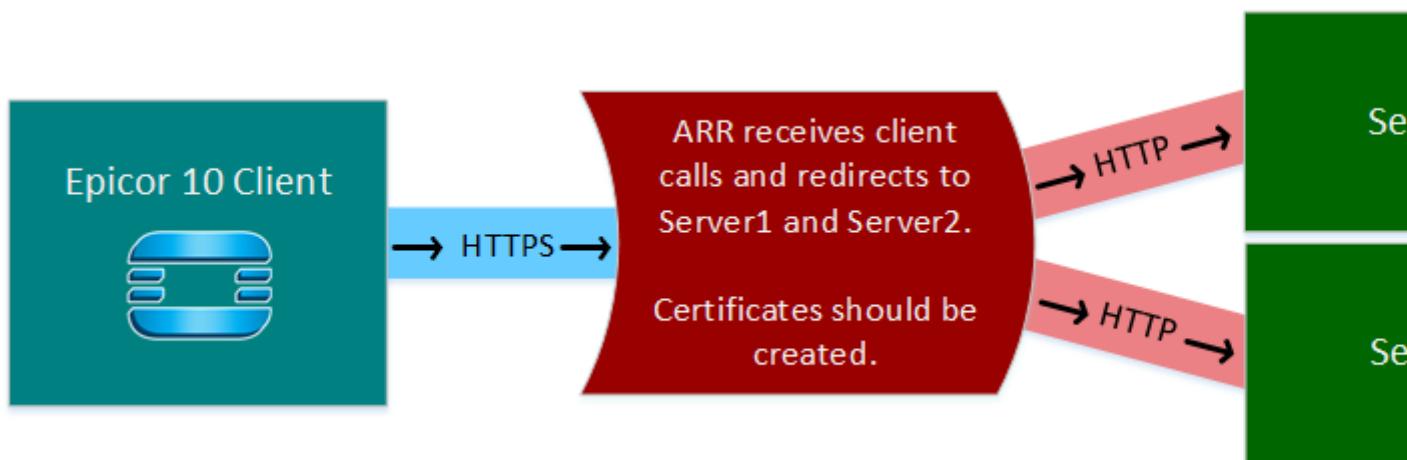
When the task agent runs, it uses the purge settings you defined.

## Configure Application Request Routing

Application Request Routing (ARR) extends Internet Information Services (IIS). This extension causes a server farm to also run as a load balancer between application servers. When ARR is installed, the server farm can route incoming message calls to multiple application servers, improving network performance and load distributes to an application server with the capacity available to process it.

ARR works with several protocol binding options. This section of the guide explores how you implement ARR with the **HttpsBinaryUserNameChannel** binding and the **HttpsOffloadBinaryUserNameChannel** binding. To use other bindings with ARR, you can follow a similar process. These instructions also describe how you set up ARR in your test environment and in your live environment.

This next graphic displays how you load balance your live system using the **HttpsOffloadBinaryUserNameChannel** protocol binding: the client sends calls to the ARR Server, and then the ARR Server distributes the calls to either Server 1 or Server 2. The connection is secured through valid signed certificates. You define which calls to send each server by creating rules.



## Install and Configure Application Request Routing

Use these steps to install and add the Application Request Routing (ARR) extension to Internet Information Services (IIS).

1. On your server machine, navigate to <http://www.iis.net/downloads/microsoft/application-request-routing>, download and install the ARR extension (if you do not have it installed).
2. Navigate to <http://www.iis.net/downloads/microsoft/url-rewrite>, download and install the URL Rewrite extension (if you do not have it installed).
3. Enable the Management Service feature in Internet Information Services (IIS) Manager (if you do not have it enabled):
  - a. Launch the **Server Manager**.
  - b. From the **Main Menu**, click **Add roles and features**.
  - c. In the **In the Before you begin dialog**, click **Next**.

- d. In the Select installation type dialog, select the **Role-based or feature-based installation** option and click **Next**.
  - e. The **Select destination server** step displays. Click the **Select a server from the server pool** radio button option, select the server, and click **Next**.
  - f. In the Select server roles dialog, expand the **Web Server (IIS) > Management Tools** node. Select the **Management Service** option. Click **Next**.
  - g. In the Select features dialog, select which features you need. Click **Next**.
  - h. Review your installation selections. If you are ready, click the **Install** button.
- 4.** Set up remote connections to your servers. To do this:
- a. On your server machine, launch **IIS Manager**.
  - b. Select your **Server** and double-click the **Management Service** icon.
  - c. Select the **Enable remote connections** check box. In the **Actions** pane, click **Apply**.
  - d. From the tree view, click the **Start Page** icon.
  - e. From the **Connection Tasks** pane, select the **Connect to a server...** option.
  - f. On the Connect to Server dialog, enter the full **Server name** and click **Next**.
  - g. The wizard indicates whether a new connection was successful. Click **Finish**.
  - h. Repeat steps D-F to add all the servers you need to load balance.
  - i. When you finish, for each added server, repeat steps B-C to enable remote connections on all servers.
- 5.** Connect Application Request Routing (ARR) to your servers. To do this:
- a. Within the **IIS Manager**, expand the **ARRServer > Server Farms** node.
  - b. Right-click this node and select the **Create Server Farm** option. Click **Yes** to the Rewrite Rules warning message to create a default rule for the farm. Your screen may look similar to the following:  

  - c. The new server farm displays as a node on the tree view.
  - d. Add the servers you need to the new web farm.
- 6.** Increase your Proxy Time-Out Value. To do this:

- a. On the ARR server, expand the **Server Farms** node. Select **Farm**.
- b. In the middle pane, double-click the **Proxy** icon.
- c. In the Proxy dialog, change the value of **Time-out (seconds)** to **10200**.
- d. From the **Actions** menu, select **Apply** to save the change.

## Create Certificates

Use these steps to create certificates which secure and authenticate the connection between the clients and the servers.

During testing you can use self-signed certificates. However when you implement ARR in your live production environment, these certificates must be valid and signed by a certificate authority. A certificate is created that connects to the ARR Server location; for example ([https://\[ARRServerName\]](https://[ARRServerName]))



**Note** When you use the **HttpsOffloadBinaryUserNameChannel** binding, the calls transport through HTTP and a certificate is not needed to communicate with the servers.

1. While you set up the Epicor application in your test environment, you can create self-signed certificates. Use these temporary certificates to ensure your network is secure and has optimal performance.
  - a. On your server machine, launch the **Internet Information Services (IIS) Manager**.
  - b. From the tree view, select the **ARR Server**. Then from the middle pane, select **Server Certificates**.
  - c. In the **Actions** pane of the Server Certificates dialog, click the **Create Self-Signed Certificate** option.
  - d. In the **Specify a friendly name for the certificate** field, enter a name for the test certificate. Be sure this name easily identifies the purpose for the certificate.
  - e. Select a certificate store for the self-signed certificate. Available options include:
    - **Personal**
    - **Web Hosting**
  - f. Click **OK**.

You can use this self-signed certificate within your test environment. Refer to the **Add a Certificate** section later in this guide for details on how to add this certificate to your server.

2. When you are ready to implement ARR in your live production environment, you must use valid signed certificates. To do this, you first request a certificate from a certificate authority and then complete the certificate request.
  - a. On your server machine, launch the **Internet Information Services (IIS) Manager**.
  - b. From the tree view, select the **ARR Server**. Then from the middle pane, select **Server Certificates**.
  - c. In the **Actions** pane of the Server Certificates dialog, click the **Create Certificate Request** option.
  - d. The **Request Certificate** wizard displays. In the **Distinguished Name Properties** step, enter details about your organization. Specify the following data:
    - **Common name**
    - **Organization**

- **Organizational unit**
- **City/locality**
- **State/province**
- **Country/region**

Once you have entered these details, click **Next**.

- e. The **Cryptographic Service Provider Properties** pane displays. From the **Cryptographic service provider** drop-down list, select from which authority you want to receive the certificate.
- f. Enter a **Bit length** for the encryption key. This value determines the security strength of the certificate. A higher value will make the certificate more secure, but it will also impact system performance. The default value is **1024**. Click **Next**.
- g. In the **File Name** wizard, enter a name that helps you identify the certificate. For example, enter ARRCert. Click **Finish**.
- h. The certificate authority generates the certificate for you. When you receive it, return to the **IIS Manager** and select the **Server Certificates** option.
- i. In the **Actions** pane, click the **Complete Certificate Request** option.
- j. In the Complete Certificate Request dialog, click the **Browse (...)** button next to the **File name containing the certification authority's response** field.
- k. Enter a **Friendly name** for the certificate. This value helps you locate the certificate in your certificate store.
- l. Use the **Select a certificate store from the new certificate** drop-down list to indicate where you want to place this certificate. Available store options include:
  - **Personal**
  - **Web Hosting**
- m. Click **OK**.

The .CER file is saved in the store you indicated. You can now use this valid certificate with your server. Refer to the **Add a Certificate** section later in this guide for details on how to add this certificate to your server.

## Set Up HttpsOffloadBinaryUserNameChannel Server

Use these steps to set up your servers for the HttpsOffloadBinaryUserNameChannel protocol binding.

When you use the HttpOffloadBinaryUserNameChannel protocol binding, you need to configure the system to use this binding and then set up the ARR Server to use HTTPS. Your application servers will then use the HTTPS protocol binding, and not an HTTP protocol binding.

1. Update the web.config file on each server. All of the load balanced servers must use the **HttpsOffloadBinaryUserNameChannel** binding.
  - a. On your server machine, open the **web.config** file. For example, navigate to C:\Epicor\ERP10\Server.
  - b. Set up the scheme setting to use the **HttpsOffloadBinaryUserNameChannel** binding:

```
<add scheme="http" binding="customBinding" bindingConfiguration="HttpsOffloadBinaryUserNameChannel" />
```

- c. Uncomment this **behavior** node:

```
<behaviors>
    <serviceBehaviors>
        <behavior>
            <AddressFilterModeAny />
```

- d. Save and exit the web.config file.
- e. Repeat these steps on each server that you want to interact with ARR.

## 2. Define the HTTPS binding values on your ARR Server:

- a. Within the **IIS Manager**, expand the **[YourServerName] > Sites > Default Web Site** node.
- b. Right-click this node and select the **Edit Bindings** option.
- c. In the Site Bindings dialog, select the **https** type. The buttons activate on the right side of this dialog.



**Note** If the https type is not available in the list, use Windows Online Help for information on how to add it.

- d. Click the **Edit** button. In the Edit Site Binding dialog, select the **IP address** for the site binding.
- e. For the **Port**, specify a port for the connection. For example, enter 443.
- f. Enter the **Host name** for the server.
- g. Optionally, select the **Require Server Name Indication** check box.
- h. From the **SSL Certificate** drop-down list, select the IP address that will use the certificate.
- i. Now select the certificate. Click the **Select** button.
- j. The available certificates appear on the Select Certificate dialog. Notice you can also search for certificates. Select the certificate you want to use and click **OK**.
- k. Click **OK** in the **Edit Site Binding** dialog.
- l. **Close** the Site Bindings dialog.

## 3. Activate HTTPS on the ARR server:

- a. Within the **IIS Manager**, right-click the **[YourServerName]** icon on the tree view and select **Stop**.
- b. After the server has stopped, right-click the **[YourServerName]** icon on the tree view again and select **Start**.
- c. Verify the server can open without any errors. Launch your browser and navigate to the **SessionMod.svc** file. For example, navigate to [https://\[YourServerName\]/\[YourEpicorInstallation\]/Ice/Lib/SessionMod.svc](https://[YourServerName]/[YourEpicorInstallation]/Ice/Lib/SessionMod.svc).

## Set Up HttpsBinaryUserNameChannel Server

Use these steps to set up your servers for the **HttpBinaryUserNameChannel** protocol binding.

When you use the HttpBinaryUserNameChannel protocol binding, you configure the system to use this binding and disable the SSL OFFload function.

1. Update the web.config file on each server. All of the load balanced servers must use the **HttpsBinaryUserNameChannel** binding.
  - a. On your server machine, open the **web.config** file. For example, navigate to C:\Epicor\ERP10\Server.
  - b. Set up the scheme setting to use the **HttpsBinaryUserNameChannel** binding:

```
<add scheme="https" binding="customBinding" bindingConfiguration="HttpsBinaryUserNameChannel" />
```
  - c. Save and exit the web.config file.
  - d. Repeat these steps on each server that you want to interact with ARR.
2. For the **HttpsBinaryUserNameChannel** protocol binding, data transactions use HTTPS instead of HTTP. To change this, disable the SSL OFFload function within the routing rules for the ARR Server.
  - a. Within the **IIS Manager**, expand the **Server Farms > ARR** node.
  - b. On the middle pane, select the **Routing Rules** icon.
  - c. On the Routing Rules dialog, clear the **Enable SSL offloading** check box. A new ARR rule is automatically created and placed at the beginning of the URL rewrite rules. This new rule contains **https://** at the beginning of its action URL. The request will now run as HTTPS on the application server.

## Configure Application Servers

Use these steps to configure your application servers for using the HTTPS binding.

You create or update the applications servers within the Epicor Administration Console. This program controls how the Epicor application interacts with the system, so it does not directly connect to AAR. Because of this, you set up the application servers to interact with the Epicor Administration Console in a different way from how the web farm interacts with the system.

To do this, set up your application servers to use the HttpsBinaryUserNameChannel protocol binding. This protocol is an intermediary binding that offloads the Secure Sockets Layer (SSL) both before and after the system can use the HTTPS binding.

1. Navigate to Epicor Administration Console.
2. In the tree view, select your **Server Management > [server] > [application server]**.
3. In the **Actions** pane, click **Application Server Configuration**.
4. Navigate to the **Application Server Settings** sheet.
5. From the **Endpoint Binding** drop-down list, select the **HttpsBinaryUsernameChannel** binding option.
6. Click **Deploy**. The application server now uses the HttpsBinaryUsernameChannel protocol binding.
7. Repeat these steps for each application server you wish to load balance.

## Add Certificates

Use these steps to add certificates to your live and test environments.

### Add Certificate for Default Website

Use these steps to add a certificate to use for Default Website in your live or test environment.

1. On your server machine, navigate to **IIS Manager**.
2. Expand the **[ARRServerName] > Sites** node. Right-click the **Default Web Site** node and select the **Edit Bindings** option.
3. In the Site Bindings dialog, select the **https** type.
4. Click the **Edit** button. On the Edit Site Binding dialog, select the **IP address** for the site binding.
5. In the **Port** field, enter a port for the connection. For example, enter 443.
6. Enter the **Host name** for the server.
7. If you need, select the **Require Server Name Indication** check box.
8. From the **SSL Certificate** drop-down list, select the IP address that will use the certificate.
9. Click the **Select** button.
10. The available certificates display in the Select Certificate dialog. Notice you can also search for certificates. Select the certificate you want to use and click **OK**.
11. Click **OK** in the Edit Site Binding dialog. The default web site for the ARR Server now uses the valid certificate you selected.

If you are setting up your live environment, your system is now load balanced using Application Request Routing. However if you are using self-signed certificates in your test environment, you need to complete the additional tasks described in the next section.

### Add Self-Signed Certificates (Test Environment)

Use these steps to add self-signed certificates to your test environment.

To use self-signed certificates in your test environment, the certificates on the ARR Server need to be exported. You then import these certificates into the client machines

1. Export the self-signed certificate from the ARR Server.  
 **Important** You can only export public key certificates (.cer files). Do not distribute self-signed certificates with private keys (.pfx files) between clients.
  - a. On your server machine, launch the **IIS Manager**.
  - b. From **ARR Server**, select **Server Certificates**.
  - c. In the center pane of the Server Certificates dialog, right-click the self-signed certificate you wish to export and select the **Export** option.

- d. In the Export Certificate dialog, indicate the directory path where you want to export the self-signed certificate. Click the **Browse (...)** button next to the **Export to** field.
  - e. In the Specify save as file name dialog, navigate to the directory path and folder you want to contain the export file.
  - f. Enter a **file name** for the self-signed certificate.
  - g. For the **file type**, select the **\*.\*** wildcard option. Click **Open**.
  - h. Enter a **Password** and then enter this password again in the **Confirm Password** field. Click **OK**. The self-signed certificate (.cer file) is exported to your selected directory file location.
- 2.** Import the self-signed certificate from the ARR Server into the Local Computer store on the client machines. This creates a secure connection between the client machines and the ARR Server in your test environment.
- a. On your client machine, from **Control Panel**, launch the **Certification Manager**.
  - b. In the tree view, expand the **Trusted People > Certificates** node. Right-click the **Certificates** node and select the **All Tasks > Import** option.
  - c. The **Welcome** step of the **Certificate Import Wizard** explains the purpose of the wizard. Click **Next**.
  - d. On the **File to Import** step, click the **Browse (...)** button to find and select the self-signed certificate (.cer file). Click **Next**.
  - e. Enter a **Password** for the certificate and click **Next**.
  - f. Review your selection and click **Finish**.
  - g. Repeat these steps on each client within your test environment.
- 3.** Verify each client installation uses the correct connection to the server. To do this, update the .sysconfig file used to launch the client.
- a. Using your explorer, navigate to the **config** folder on your client installation. For example, C:\Epicor\{EpicorVersion}\Client\config.
  - b. Open the **.sysconfig** file in a text editor like **Notepad**.
  - c. Update the following settings:
    - If you use **HttpsOffloadBinaryUserNameChannel**, enter

```
<AppServerURL value="https://[YourARRURL]" />
<EndpointBinding value="HttpsOffloadBinaryUserNameChannel" />
```
    - If you use **HttpsBinaryUserNameChannel**, enter

```
<AppServerURL value="https://[ YourARRURL ]" />
<EndpointBinding value="HttpsBinaryUserNameChannel" />
```
  - d. Save the .sysconfig file.
  - e. Now launch the Epicor client to verify it displays.
  - f. Repeat these steps on each client in your test environment.

4. If you use the **HttpsBinaryUserNameChannel** protocol binding, you next create self-signed certificates on each server machine. Because your test environment uses an HTTPS protocol, the system needs these certificates to ensure the security of the connection.
  - a. On your server machine, launch **IIS Manager**.
  - b. Create a self-signed certificate for the test environment. From the tree view, select the **[YourServerName]** node. Then from the middle pane, select **Server Certificates**.
  - c. In the **Actions** pane of the Server Certificates dialog, click the **Create Self-Signed Certificate** option.
  - d. In the **Specify a friendly name for the certificate** field, enter a name for the test certificate. Be sure this name easily identifies the purpose for the certificate.
  - e. Now select a certificate store for the self-signed certificate. Available options:
    - **Personal**
    - **Web Hosting**
  - f. Click **OK**.
  - g. Repeat these steps for each server you want to load balance in your test environment.
5. Export the self-signed certificate you created on each server machine.

 **Important** You can only export public key certificates (.cer files). Do not distribute self-signed certificates with private keys (.pfx files) between clients.

  - a. In **IIS Manager**, from the **[YourServerName]** node, select **Server Certificates**.
  - b. In the center pane of the Server Certificates dialog, right-click the self-signed certificate you wish to export and select the **Export** option.
  - c. In the Export Certificate dialog, indicate the directory path where you want to export the self-signed certificate. Click the **Browse (...)** button next to the **Export to** field.
  - d. In the Specify save as file name dialog, navigate to the directory path and folder you want to contain the export file.
  - e. Enter a **file name** for the self-signed certificate.
  - f. For the **file type**, select the **\*.\*** wildcard option. Click **Open**.
  - g. Enter a **Password** and then enter this password again in the **Confirm Password** field. Click **OK**. The self-signed certificate (.cer file) is exported to your selected directory file location.
  - h. Repeat these steps for each server you want to load balance in your test environment.
6. Import the server certificates into the ARR Server. The ARR Server runs as a client machine to the servers, so the ARR Server needs to trust these servers through a self-signed certificate. To do this:
  - a. In **IIS Manager**, from the **ARR Server**, select **Server Certificates**.
  - b. In the **Actions** pane of the Server Certificates dialog, click **Import**.
  - c. In the Import Certificate dialog, either enter the **Certificate** name or click the **Browse (...)** button to find and select the exported certificate.
  - d. If the certificate was exported with a password, enter this **Password** value.

- e. If you want to export this certificate again, select the **Allow this certificate to be exported** check box. Click **OK**.
- f. Repeat these steps to import the server certificates for each server you wish to load balance.

Because the client machines are connected to the ARR Server, they do not need the certificates from the servers. The client machines instead trust the ARR Server's certificate, so these connections are secure.

Your test environment is now load balanced using Application Request Routing.

## Manage Load Balance

Use these steps to manage load balance.

Once you have configured ARR to connect with the binding, you can then route all calls from a specific area of the Epicor application to a single server farm. This load balances the calls made against the system by pushing these specific calls out to a server farm designated to handle them.

### Route Specific Calls to Server Farm

Use these steps to route specific calls to a server farm.

This example illustrates a configuration where one server farm, **ARRMain**, has two application servers as members. To load balance this system, you will next set up another server farm with one application server that will only process calls from the SalesOrder service. This reduces the calls sent to the **ARRMain** server farm.

1. Launch **Internet Information Services (IIS) Manager**. Under the **Server Farms** node, the **ARRMain** server farm displays.
2. From the tree view, right-click the **Server Farms** icon and select **New Server Farm**.
3. Create a server farm named **ARRSales**.
4. You are asked if you want to create the **Rewrite Rule** for the new server farm. Click **No**; you will instead manually create this rule.
5. The **ARRMain** server farm is currently processing all Epicor calls regardless from which source service they originate. To route specific service calls to the **ARRSales** farm, you manually create a rule. Click on the **ARRSales** server farm icon.
6. Now from the **Actions** pane, select **Blank Rule**.
7. In the **Blank Rule** dialog, you first set up the **Match URL**. From the **Requested URL** drop-down list, select the **Matches the Pattern** option.
8. You first set up the **Match URL**. From the **Requested URL** drop-down list, select the **Matches the Pattern** option.
9. From the **Using** drop-down list, select the **Wildcards** option.
10. Enter the **Pattern**. This limits the calls to the server to a specific service. For this example, enter \*erp/bo/SalesOrder.svc; this server farm will only receive calls from the SalesOrder service.
11. To handle this example, you set up one condition. From the **Logical grouping** drop-down list, select **Match All**.

12. Click the **Add** button. For the **Input** protocol, select **HTTPS**.
13. Now for the **Action**, indicate you want all Sales Order calls to go to the **ARRSales** server farm. From the **Action Type** drop-down list, select **Route to Server Farm**.
14. For the **Scheme**, select the **https://** option.
15. Click the **Server farm** drop-down list and select the **ARRSales** option.
16. Select the **Stop processing of subsequent rules** check box. This indicates only calls from the Sales Order Entry service are sent to the **ARRSales** server farm.
17. Prevent the **ARRMain** server from processing sales order calls.
  - a. Click the server and select the **Rewrite Rule** option. Click **Edit**.
  - b. Expand the **Conditions** section and click the **Add** button.
  - c. From the **Check if input string** drop-down list, select **Does Not Match the Pattern**.
  - d. Now for the **Pattern**, enter **SalesOrder**.
  - e. Select the **Ignore case** check box. **Save** the rule change.

## Test Load Balance

Use these steps to test the load balance.

Through this test, you can see if the calls sent from the SalesOrder service are routing to the server within the **ARRSales** server farm.

1. Log into the **Epicor ERP** application.
2. Navigate to **Order Management > Sales Order Management > General Operations > Project Entry**.
3. Click **New Project** and then click **Clear**. Repeat this step several times.
4. Return to **Internet Information Services (IIS) Manager**.
5. Click on the **ARRMain** server farm. The **Monitoring and Management** pane displays. Notice the service call messages display for Project Entry.
6. Return to the **Epicor ERP** application.
7. Navigate to **Order Management > Sales Order Management > General Operations > Sales Order Entry**.
8. Click **New Order** and then click **Clear**. Repeat this step several times.
9. Return to **Internet Information Services (IIS) Manager**.
10. Click on the **ARRMain** server farm. The **Monitoring and Management** pane displays again. Notice the **ARRMain** server farm does not receive sales order calls.
11. Now select the **ARRSales** server farm. Once again the **Monitoring and Management** pane appears, notice the sales order message calls display.

The sales order calls now only run on the ARRSales server farm, while all other calls run on the AARMain server farm. You can continue to add more rules to further balance the load between the two server farms.

# Manage Epicor ERP

---

This section of the user guide explores the tools and techniques you can use to manage the Epicor ERP application.

This part of the guide begins by documenting the options available for securing the Epicor ERP application. You can define complexity requirements for user account passwords to help prevent malicious access. For secure ease of entry, you can set up user accounts to automatically log into the application. If users incorrectly enter their user name/password combinations, you may also create an account lockout policy that temporarily freezes the account. The Epicor ERP application also has a series of programs you can leverage to control access to the user interface. By assigning users to security groups, you can prevent/grant access to specific programs based on each user's role in your organization.

This section next explores how you configure client installations. You can modify these files to define startup parameters. When users launch their client installations, these startup parameters activate. For example, you can set up a configuration settings file so users automatically log in with their user account. Similarly you can define run time arguments on Epicor ERP shortcut items. Use these run time arguments to cause a shortcut icon to launch with the MES interface, open to a specific menu, use a custom configuration settings file, and so on.

The middle part of this section explores the management features contained within the Epicor ERP application. For example, you can set up schedules that users can then select on reports, processes, and executive queries. When the system clock activates the schedule, the items linked to this schedule automatically run.

The Epicor ERP application also has a number of programs that manage specific areas of the application. For instance, you use the Conversion Workbench to handle database conversions. If an individual leaves your organization, use the Personalization Purge to remove all the personalization layers linked to this user account. These management programs are described briefly at the end of this section so you can learn about the purpose of these key tools.



**Tip** For information on improving performance, review the Performance Tuning Guide. This companion guide is also in the application help under the **System Management > Working With System Management** node.

## Authentication - User Identity Security

---

Controlling access to the application is one of the primary ways you can secure the Epicor ERP application. When you authenticate the identity of users attempting to login, or call, the application, you help prevent malicious access.

You authenticate user identity through the following methods. These methods have both advantages and disadvantages, so select the method that works the best for your organization:

- **Windows Account** - Use this method to authenticate user identity through Windows accounts when the client and servers are on the same Windows Domain. These accounts are secured by the Windows operating system, making it much more difficult for these accounts to be externally compromised.

This method controls access at the operating system level, so you can define your password policy and account lockout policy through the Group Security Policy program. This method is easier to administrate, as you control access at the operating system level. If an administrator disables a Windows Domain account, the user will have no access to Epicor ERP. The disadvantage to this method is that if malicious users do compromise your Windows environment, they gain access to all applications on your system.

- **Epicor Account** - If you use this method, you authenticate user identity through your internal Epicor accounts. You then control access at the application level, using both the Password Policy Maintenance and Account

Lockout Policy programs to define the complexity of passwords and the number of failed logon attempts you allow.

Like Windows accounts, your Epicor accounts are encrypted. By securing at the application level, you make it harder for malicious users to specifically access Epicor ERP. However the disadvantage to this method is users will need to manage separate passwords for each application in your environment, making it harder for you to administrate security. The following sections describe how you implement authentication security through either method.

- **Azure AD Identity** - Use this method to authenticate user identity when you manage Windows accounts through Microsoft® Azure® Active Directory (Azure AD). Azure AD is Microsoft's multi-tenant, cloud based directory. It provides centralized identity management service not only in your on-premise domain, but also across the internet, giving users easy access to corporate cloud-based applications.

The advantage of Azure AD authentication is that user accounts are secured by Azure, making it much more difficult for these accounts to be externally compromised. This method controls access within Azure, so you can define your password policy and account lockout policy centrally for internal and external applications. The disadvantage to this method is that if malicious users do compromise your identity, they gain access to all applications in your system. There are advanced security and monitoring services Administrators can opt into, such as self-service password management, multi-factor authentication, AI based Identity Monitoring and Identity Protection.

 **Note** A user can have multiple identities. All of the above mentioned methods: Epicor UserName / Password, a Windows Domain Identity and an Azure AD identity can be mapped to the same Epicor User.

## Epicor Account Authentication

This section describes what you need to set up and configure when you authenticate user identity through internal Epicor accounts.

### Password Policy Maintenance

Use Password Policy Maintenance to determine the complexity requirements for user account passwords. Each new or updated password users enter must follow the requirements you define in this program.

You start by indicating how many characters each password needs before the system accepts it. You then activate other options as well, such as whether the password requires uppercase letters, must contain special characters, and/or allow user account names.

After you save these options, these password requirements activate. The next time users create or change passwords, they must enter values that follow these complexity requirements.

**Menu Path:** System Setup > Security Maintenance > Password Policy

### Define Password Policy

You can select the following password complexity requirements.

1. Enter the **Minimum password length** for each password. The Epicor ERP application then only accepts passwords at least this length or longer.
2. Select the **Allow include user ID** check box to indicate users can enter their user account identifiers in passwords. They can then enter passwords based all or in part from their User IDs.
3. Select the **Allow include user name portion** check box to grant users the ability to enter all or part of their user account names for their passwords. Users can then enter passwords based on their user account names.

4. However when you **do not** select the Allow include user name portion check box, the **Match length** field is active. You enter a numeric value in this field to define the top limit on how many characters from the user account name can be included in the password.

For example if you enter 4 in this field, the policy only allows a sequence of three characters or less from the user account name. If the user name is BHarris, then a new/updated password for the user account can only contain "ris", "BHa", "Har", or similar character sequences.

5. You can also indicate that each password must contain at least one character from one or multiple **Character categories**. For example, if you select the **Require uppercase** check box, each new or changed password must have at least one uppercase English (A-Z) character.
6. Use the **Minimum categories** field to define how many character categories such as lowercase, uppercase, and so on must be present in each password. Instead of requiring specific categories, use this option to indicate that each password must contain at least this many character types. This method gives users flexibility, as they can then decide which character types to use within their passwords.

 **Tip** You can use this feature and still require some specific character categories like lowercase, uppercase, and so on be included on each password. Users then must enter passwords that contain these required character categories, but also include other character categories they choose. This gives users partial flexibility while still requiring some specific categories.

7. Use the **Allow blank password** check box to control whether Security Managers should be allowed to reset user passwords to a temporary value of blank.

When this check box is selected, Security Manager can set a user password to blank, so users are allowed to log in up to three times with the blank password. Each time they login with the blank password they are prompted to create a password that conforms to password policy. If they do not create a conforming password after three logins, they are locked out until System Manager again resets their password.

If you keep this checkbox cleared, when a Security Manager clicks the **Reset Password** button in **User Account Security Maintenance** for an existing user or saves a new user, the Set Temporary Password dialog does not allow the Security Manager to reset the user's password to blank. Instead, a temporary password is generated and e-mailed to either the e-mail address on the user record or an e-mail address entered immediately by the Security Manager. For more information, review the Password Management topic.

8. When you finish setting up the password policy, click **Save**.

## Expire All Passwords

You run the Expire All Passwords option to expire all current passwords on active user accounts. Use this process when you have created or updated the password policy and you need all passwords to comply with the current requirements.

To expire all passwords:

1. Click the **Actions** menu.
2. Select the **Expire All Passwords** option.
3. You are asked if you want to expire all passwords; click **Yes**.

Now all users have three logins to update their passwords. Their old passwords still work during these three logins, but after they use up these grace logins their old passwords no longer grant access. This forces all users to create new passwords that follow your current policy requirements.



**Tip** If you are a Security Manager, you can expire all passwords except those linked to Global Security Manager accounts. If you are a Global Security Manager managing a SaaS hosted environment, you will expire all passwords in the current tenant.

System administrators grant Epicor user accounts global security manager rights within the Epicor Administration Console or within **User Account Security Maintenance** on the **List** sheet. For more information, review the application help for the **Epicor Administration Console**.

## Special Characters List

The following table contains the special characters available to use in passwords. When you require special characters on your password policy, users must include at least one of these characters on their passwords.

!	)	;	]
"	*	<	^
#	+	=	-
\$	,	>	`
%	-	?	{
&	.	@	
:	/	[	}
(	:	\	~

## Password Management

You manage passwords individually on each user account. You can expire an individual password, clear a password, and enter how long each password can be used.

### Password Options

You control passwords through User Account Security Maintenance.

**1. Launch **User Account Security Maintenance**.**

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

**2. Find and select the user record you need to review.**

**3. Click the **Expire Password** button to force the user to enter a new password the next time he or she logs into the application.**

**4. If you click the **Reset Password** check box instead, the Set Temporary Password dialog is displayed where you can either accept the retrieved e-mail address (if any) associated with user account or enter an alternate e-mail address to send the temporary password to. When you click **OK**, the system generates a temporary password and e-mails it to the user. The user can login using the temporary password up to three times and each time will be prompted to enter a conforming password to replace the temporary password.**

You can also select the **Set temporary password to blank** check box. When you allow blank password, users have three login attempts with blank password and each time they are prompted to enter a proper password.



**Note** This option is only available if **Password Policy Maintenance** is set up to allow blank passwords. You control this setting by the **Allow blank password** check box.

5. The **Date last Used** field displays the most recent day on which the password on the current account was used to access the Epicor ERP application.
6. The **Password Last Changed** field displays the date on which the current user most recently change the password on this account.
7. The **Password Expires** field displays the date on which the current password on this user account will expire.
8. Use the **Password Expires Days** field to indicate how many days from when a password is entered or changed before it will expire. You typically enter a date in this field when you select the Expire Password check box.
9. When you finish managing the password on this user account, click **Save**.

## Account Lockouts

You can further secure access to the Epicor ERP application by defining an account lockout policy. When users repeatedly fail to log into the application, their accounts become inactive, or locked, for a period of time you determine.

You set up the lockout policy for your organization through the Account Lockout Policy program. You define both how many failed attempts the application will allow and how long the account is locked. Then while a user account is locked, you can launch User Account Security Maintenance to review how long the account is locked and if you wish, manually unlock this user account. You can also unlock accounts through the Epicor Administration Console.

## Account Lockout Policy

Use the Account Lockout Policy program to define what happens when users fail to log into the Epicor ERP application with their correct user account name/password combination.

These fields determine the overall lockout policy for all user accounts within either a server-client based environment or the current tenant in a SaaS or similar hosted environment. You first indicate how many attempts users can try before they are locked out. You also define how long users are locked out of the Epicor ERP application; you can prevent users from logging in for a specific time duration or an ever increasing time duration. When the system clock passes this time limit, users can attempt to login again through their user accounts.

After you save these lockout settings, this policy activates the next time users log into the Epicor ERP application. When they fail to log into the application, an error message displays indicating for how long they will be locked out of their accounts.

**Menu Path:** System Setup > Security Maintenance > Account Lockout Policy

### *Create the Policy*

Follow these steps to create your account lockout policy.

1. Click **New**.
2. Define how many times a user can incorrectly attempt to access the application by entering a value in the **Lockout Threshold (attempts)** field.

3. Now within the **Reset Counter After (minutes)** field, determine how many minutes can pass before the failed attempts counter resets. If the user does not attempt to log in until the system clock passes this duration of time, the attempts counter returns to zero and the user can log in using the available attempts defined by the **Lockout Threshold** value.
4. If the user surpasses the number of login attempts allowed by the **Lockout Threshold** value, the user account is locked for a duration of time. You indicate how long the user is locked out through these options:
  - **Lockout Duration** - Defines a specific value, in minutes, a user account is locked before it can be used again to log into the Epicor ERP application.
  - **Incremental Lockout** - Select this check box to indicate the system will lock the user account for longer and longer time periods. The system tracks each failed attempt and then doubles the time delay. The user is first locked out for 1 second, then 2 seconds, then 4, 8, 16, 32, 64, and so on.
5. When you finish setting up the lockout policy, click **Save**.

The next time users log into the application, this lockout policy is active.

If you need to change the lockout policy, access the **Account Lockout Policy** program again. Update the values you need and click **Save**. The updated lockout policy values are now active. They are enforced the next time users log into the Epicor ERP application.

## Locked Accounts

When users fail to log into the application, their accounts become inactive, or locked. Users are unable to access these accounts until the specific or incremental time limit expires.

To find out which user accounts are locked, use the System Activity Log. The grid on this dashboard records when a user fails to access the Epicor ERP application. You can then see the User ID for the account and when the lockout happened.

You typically unlock accounts by launching User Account Security Maintenance. You can see how long this account will be locked and also manually re-activate this account. When user accounts become locked, you should use this program to activate them again.

However you can also unlock accounts through the Epicor Administration Console. While you can unlock all accounts through the Epicor Administration Console, this feature is most useful when you accidentally lock out a security manager or global security manager account. Because you cannot restore these types of accounts inside the Epicor ERP application, you need to instead unlock them on the server.

### Track Locked Accounts

Use the **System Activity Log** dashboard to see which user accounts are locked and when the lockout occurred.

The System Activity Log captures all database modifications that happen in the Epicor ERP application. Use this tool to find out where and when specific database changes were done and who did them. If a user attempts to login greater than the number of failed attempts you allow, the user account locks and an entry appears in the System Activity Log. You can see the identifier for the locked account and then reactivate this account in User Account Security Maintenance.

To locate these entries, sort the results by **Activity Type** and find the **Log on failure** entries. You then identify the **UserID** for the locked user account and the date/time (**LastActivityOn**) the account was locked.

**Menu Path:** System Setup > Security Maintenance > System Activity Log



**Tip** To use this log, you first need to activate it within **Company Maintenance**.

## *Unlock Accounts (Account Level)*

When a user account is locked, you can activate it again through an option within User Account Security Maintenance. You typically use this feature to re-activate locked accounts.

### **1. Launch **User Account Security Maintenance**.**

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

### **2. On the **Detail** sheet, find and select the locked user record.**

**3. The **Locked Out** check box** indicates whether the current user account is locked, preventing the user from logging in through this account.

**4. The **Locked Out Until** field** displays the date on which this locked user account will activate again.

**5. Now review the **Consecutive Logon Failures** field;** this field displays how many times a user attempted and failed to log into the Epicor ERP application through this user account. These attempts occurred consecutively, and so these failed attempts caused the current user account to lock.

**6. To activate the user account again, click the **Actions** menu and select the **Unlock User Account** option.** The user account record is unlocked. The user can now attempt to log in again through this user account.

### **7. Click **Save**.**

## *Unlock Accounts (Server Level)*

You can also unlock a user account through the Epicor Administration Console.

While you can unlock all user accounts through this feature, you should only use this option when a security manager or global security manager user account is locked.

**1. Access your server machine.**

**2. Launch the **Epicor Administration Console**.**

**3. Expand the **Database Server Management** node and <YourDatabaseServer> node.**

**4. Select the database that contains the user account you need to unlock.**

**5. You can now unlock a selected user account. You can do this in the following ways:**

**a. From the **Actions** pane, select the **Unlock User Account** option.**

**b. Click **Action > Unlock User Account**.**

**c. Right-click the database; from the context menu, select **Unlock User Account**.**

The **Unlock Account** window displays.

**6. Enter the **User ID** for the account you need to unlock.**

**7. Click **OK**.**

The **Work-In-Progress** window displays. After the account is unlocked, this window closes.

The user account unlocks. You can now use this security manager account again to log into the Epicor ERP application.

## Automatic Sign On

As part of the password policy functionality, you can give users the ability to set up their Epicor user accounts to automatically sign into the application. When users launch the Epicor ERP application, they then bypass the logon window to directly access the menu.

When you activate this functionality, you create an encrypted login account that only works on the user's client installation.



**Important** This automated login option only work within environments where you control access through the User Name authentication protocols (Epicor user accounts). You cannot use automated login within environments that use token authentication, Windows Channel authentication, or Secure Sockets Layer (SSL) Channel authentication protocols.

### Allow Automatic Sign On

You activate this functionality through a check box on Password Policy Maintenance.

To allow single sign on for Epicor user accounts:

1. Launch **Password Policy Maintenance**.

**Menu Path:** System Setup > Security Maintenance > Password Policy

2. Select the **Allow save password** check box.

3. Click **Save**.

4. Now when each user logs into the Epicor ERP application, they can decide whether they want to set up their client installation to automatically launch on the **Preferences** window. Depending on the interface style, users launch this window in different ways:

a. **Classic Menu** - From the **Main Menu**, click **Options > Preferences**.

b. **Modern Shell Menu** - From the **Home** screen, click the **Settings** tile. Verify **General Options** is highlighted and click the **Preferences...** link.

The **Preferences** window displays.

5. To activate single sign on for their Epicor accounts, users select the **Automatically sign on** check box.

**Note** If you do not select the Allow save password check box on Password Policy Maintenance, the Automatically sign on check box is not available on this window.

6. The users then click **OK**.

This causes the client installation to save the user name and password. The user's password is also encrypted to prevent malicious entry.

7. The next time these users launch their client installations, they automatically log into the application.

## Windows Account Authentication

This section describes what you need to set up and configure when you authenticate user identity through Windows accounts.

### Password Policy (Windows)

You define password complexity for Windows accounts through the Local Group Policy Editor program. The complexity requirements you define here are also similar to the options for Epicor user accounts.

In contrast to Epicor accounts, the password policy you define on this program affects all Windows accounts. Any user who attempts to log into your system (instead of just the Epicor ERP application) will need to create passwords that follow these complexity requirements.

1. Access your server and use the **Search** field to find and select **Local Group Policy Editor**.
2. From the tree view, expand the **Windows Settings > Security Settings > Account Policies** node.
3. Select the **Password Policy** node.
4. The available password complexity options display in the **Policy** pane.
5. Right-click one of the policy options; from the context menu, select **Properties**.
6. The **<PolicyOption> Properties** window displays.
7. Enter the password the value you need. In this example, you are modifying the minimum length of the Windows account password.
8. Click **OK**.

The next time users need to create a new password, it must follow these complexity requirements.

### Account Lockout Policy (Windows)

You also define the account lockout policy for Windows accounts through the Local Group Policy Editor program. The lockout policy options you define here are similar to the options for Epicor user accounts.

As described previously, the account lockout policy you define on this program affects all Windows accounts. Any user who fails to log into their client machines will be locked out of the entire system (instead of just the Epicor ERP application).

1. Click your **Start** button; use the **Search** field to find and select **Local Group Policy Editor**.
2. From the tree view, expand the **Windows Settings > Security Settings > Account Policies** node.
3. Select the **Account Lockout Policy** node.
4. The available lockout policy options display in the **Policy** pane.
5. Right-click one of the policy options; from the context menu, select **Properties**.
6. The **<LockoutPolicyOption> Properties** window displays.

7. Enter the lockout policy value you need. In this example, you are modifying the lockout threshold for all Windows accounts.

8. Click **OK**.

Now the next time users repeatedly fail to log into the Windows system, they will be locked out when they pass this threshold limit.



**Note** For more information on both the password policy and the account lockout policy for Windows accounts, review your Microsoft Windows documentation.

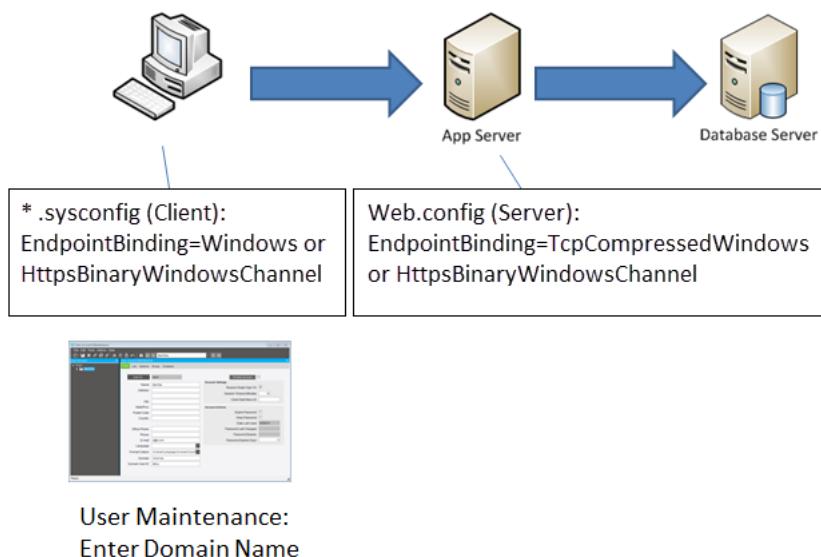
## Single Sign-On (Windows Authentication)

Single Sign-On (SSO) is a time-saving feature you implement so users can sign on (log in) using an authentication method different from standard logon with Epicor ERP user name and password. Alternative authentication methods include operating system (Windows, Unix, etc.), Azure Active Directory (AD), Epicor Identity Provider (IdP) authentication, or even an Epicor token. When you enable this feature, users no longer see a Logon window when they launch Epicor ERP; instead the Main Menu screen displays.



**Important** This automated login option only works within environments where you control access through the User Name authentication protocols (**Windows** Net.Tcp or **HttpsWindowsBinaryChannel** Https bindings).

You can set up the Single Sign-On feature for Windows authentication. To do this, you need to configure the client, server, and application server to authenticate through Windows.



**Tip** The Epicor ERP application does not support using Windows impersonation of the client application server for database access. You can use either SQL Server Authentication or Windows Authentication, but Windows Authentication identifies the Information Internet Services (IIS) application pool. The client user does not identify the application pool.

These instructions assume the Epicor ERP application is already installed on the server and client workstations.

## Epicor ERP Setup

You first set up a user account to use the Windows domain account.

1. Log into the Epicor ERP application using a security manager account.

2. Launch **User Account Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

3. Find and select the user record for which you will activate Single Sign-On (SSO) functionality.

4. Verify the **Detail** sheet displays.

5. Enter the **Domain** the user accesses to log into the computer.

6. Now enter this user's **Domain User ID**.



**Tip** When users log on through Single Sign-On, the Epicor ERP application only uses this Domain User ID for the log in value. The account password is ignored. Because Windows validates the password when the user first logs into the client machine, the application only needs the Windows identity (Domain) User ID to determine whether the account can access the system.

7. When you select the **Require Single Sign-On** check box, you indicate this user account is restricted to only use Single Sign On for logging into the Epicor ERP application.

Select this check box when:

- The user will access the server through Windows Authentication.



**Note** This functionality can also be used for other authentication methods like Azure AD, Epicor IdP, or even Epicor token.

- The server runs one single authentication method for all application servers.

DO NOT select this check box when:

- The server is configured for multiple application servers that use different authentication methods. For example, if one application server uses Windows authentication while another application server uses UsernameToken via SSL authentication, do not select this check box.
- The user logs in through different authentication methods in different environments. For example, if the user logs in through Windows authentication at the office but logs in through UsernameToken via SSL authentication while working remotely without a VPN connection, do not select this check box.

8. Click **Save**.

Repeat these steps for each user account that will use Single Sign-On.



**Important** If you use one application server, all users must be set up with the SSO login feature.

## Server Configuration

Verify the web configuration file for the application server uses the Windows TCP binding configuration.

1. Access the Epicor server.
2. Launch **Windows Explorer**.
3. Navigate to the `\inetpub\wwwroot\<name_of_Epicor_appserver>\` directory.
4. Using a text editor like **Notepad**, open the **web.config** file.
5. Locate the line that begins with `<add scheme=`".
6. Modify this setting to display the following:  
`<add scheme="net.tcp" binding="customBinding" bindingConfiguration="TcpCompressedWindows" />`  
The server is now configured to use Windows authentication.
7. **Save** your changes.
8. **Close** the text editor.

## Administration Console Setup

The application server must be configured to use the Windows account. You update these properties in the Epicor Administration Console.

When an application server uses the Windows account, its task agent also uses this account to process the tasks users activate on client workstations.

1. On your server, launch the **Epicor Administration Console**.
2. Use the tree view to navigate to the application server. Expand the **Server Management** node, and then the **<ServerName>** node.  
The application server(s) display.
3. Right-click the application server you need to change; from the context menu, select **Properties**.  
The **<ApplicationServerName> Properties** window displays. This window defines how the Epicor Administration Console connects to the application server.
4. Click the **Binding** drop-down list and select the **Windows** option.
5. Now enter the **Epicor User Name** for the Windows account. Be sure to enter this value using the **<Domain>/User Name** format.  
 **Important** In some versions of Epicor ERP, you do not need to enter the Epicor User Name and Password. The Windows account you set up on the server is automatically used, so these fields are inactive.
6. Enter the **Password** for this Windows account.
7. Click **Apply** and then click **OK**.

The application server now uses the same Windows account as the server.



**Tip** The next time you display the <ApplicationServerName> Properties window, the Epicor User Name and Password will be blank, as the application server incorporates this account as a default property.

## Client Configuration

To complete the setup, you now update the configuration settings (.sysconfig) file on each client installation.

**1.** Access the Epicor client workstation.

**2.** Launch **Windows Explorer**.

**3.** Navigate to the **Epicor ERP client** folder; open the **Config** folder.

**4.** Using **Notepad** or a similar text editor, display the **[AppServerName].sysconfig** file. This configuration file defines the settings that activate when the user launches the Epicor ERP client application.

**5.** Locate the setting that begins with `<EndpointBinding value=`.

**6.** Modify this setting to display the following:

```
<EndpointBinding value="Windows" options="UsernameSslChannel|Windows|Userna  
mewindowsChannel" />
```

The Epicor ERP client is now configured to use Windows authentication.

**7.** If you are making the Single Sign On feature mandatory for all users, locate the setting that begins with `<SingleSignOn value=`.

**8.** Change this line to display: `<SingleSignOn value="true" bool="" />`

**9.** **Save** your changes.

**10.** **Close** the text editor.

**11.** Test the setup by double-clicking the Epicor ERP client icon.

The logon window no longer displays; the application launches directly to the Menu screen.

## Azure AD Authentication

Epicor ERP enables authentication of ERP application users against users in Microsoft® Azure® Active Directory (Azure AD).

Azure AD is Microsoft's multi-tenant, cloud based directory. It provides centralized identity management service not only in your on-premise domain, but also across the internet, giving users easy access to corporate cloud-based applications. Azure AD also offers a rich, standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules.

The advantage of Azure AD authentication is that user accounts are secured by Azure, making it much more difficult for these accounts to be externally compromised. This method controls access within Azure, so you can define your password policy and account lockout policy centrally for internal and external applications. There are advanced security and monitoring services Administrators can opt into, such as self-service password management, multi-factor authentication, AI based Identity Monitoring and Identity Protection.

Azure AD stores user identities for an Enterprise. For multi-tenant scenarios, an Enterprise is mapped to a Tenant ID in ERP 10. To work against Azure AD, a user must authenticate against the Azure AD and obtain a token to be passed to the ERP 10 Server as identification.

To support the Azure AD authentication as the source, Epicor ERP uses dedicated bindings which are configurable in Epicor ERP 10 Admin Console.

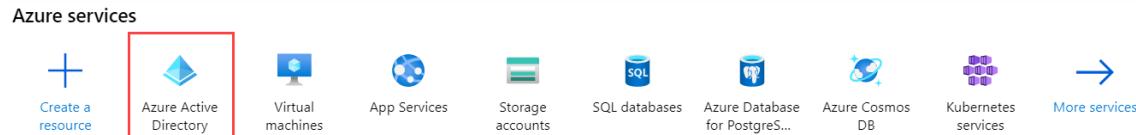
In this section, learn how to implement authentication of ERP application users against Azure AD.

## Configure Azure Portal

These steps discuss the initial Azure Active Directory authentication setup, which includes obtaining of your Azure Tenant ID and registration of server and client applications.

### Obtain Azure Tenant ID

1. Log into the Microsoft® Azure® portal <https://portal.azure.com>.
2. From the Tree-view, select **Azure Active Directory**.



3. Click on **Properties** and take note of the **Directory ID** value.

The screenshot shows the 'Directory properties' page for an Azure Active Directory tenant named 'Epicor'. The left sidebar has a 'Properties' item selected, indicated by a blue highlight. On the right, there are fields for 'Name' (Epicor), 'Country or region' (United States), 'Location' (United States datacenters), 'Notification language' (English), and 'Directory ID' (a long GUID). A red arrow points to the 'Directory ID' input field.

You enter this value in **Azure Active Directory Settings Maintenance** form, in **Azure Active Directory ID** field. In ERP 10 application's sysconfig, this value needs to be specified in the **AzureADDirectoryID** setting.

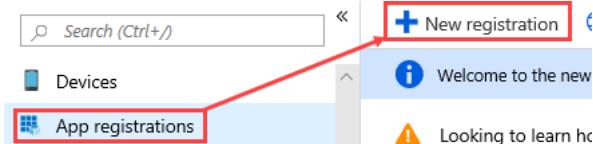
**Example** <AzureADDirectoryID value="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" />

**Tip** The process of updating .sysconfig files is explained later in this section.

## Register Server Application

Now create the **application for the Epicor server installation**. This application is used by server-side and JS applications, like **Kinetic Home Page**.

1. Click on **App registrations** and select **+ New registration**



2. Enter a **Name**. You may use the format of <ApplicationName> + **Server** - for example, **ERP102x00Server**.
3. Keep the default option in the **Supported account types** section.
4. From the **Redirect URI** type drop-down, select **Public client/native (mobile & desktop)**. For the URI, enter the Home page address of your Epicor ERP application, in the format of **https://<server>/<applicationname>/home/**, for example **https://server/erp102x00/home/**. This address becomes the first Redirect URI for this application registration. This is where a user is directed when launching Epicor ERP with Kinetic Home Page or when accessing Kinetic Home Page from within a browser.

## Register an application

### \* Name

The user-facing display name for this application (this can be changed later).

ERP102x00Server

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Epicor only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional, but a value is required for most authentication scenarios.

Public client/native (mobile ... ▾

https://server/erp102x00/home/





**Important** Azure AD Redirect URIs are case-sensitive, be sure to use **lowercase** for this URL as shown above.

## 5. Register the application.

The newly registered application overview page displays.

Home > Epicor - App registrations > ERP102400Server

ERP102400Server

Search (Ctrl+ /)

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Display name	: ERP102400Server	Supported account types	: My organization only
Application (client) ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Redirect URIs	: 1 web, 0 public client
Directory (tenant) ID	: 00000000-0000-0000-0000-000000000000	Managed application in...	: ERP102400Server
Object ID	: 00000000-0000-0000-0000-000000000000		

Call APIs

Documentation

Microsoft identity platform  
Authentication scenarios  
Authentication libraries  
Code samples  
Microsoft Graph  
Glossary  
Help and Support

View API Permissions

Manage

- Branding
- Authentication
- Certificates & secrets
- API permissions
- Expose an API** (highlighted with a red arrow)
- Owners
- Manifest

Support + Troubleshooting

Troubleshooting

New support request

## 6. Take note of the of the **Application (client) ID** value.

You enter this value into the **Web Application ID** field in the **Azure Active Directory Settings Maintenance** program. In the client .sysconfig, this value needs to be specified in the **AzureADWebAppID** setting.



**Example** <AzureADWebAppID value="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" />

## 7. In the left-side **Manage** navigation panel, click **Expose an API**.

## 8. In the **Scopes defined by this API** section, click the **Add a scope** button.

Home > Epicor - App registrations > ERP102400Server - Expose an API

ERP102400Server - Expose an API

Search (Ctrl+ /)

Application ID URI Set

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

+ Add a scope (highlighted with a red arrow)

SCOPES	WHO CAN CONSENT	ADMIN CONSENT DISPLAY NAME	USER CONSENT DISPLAY N
No scopes have been defined			

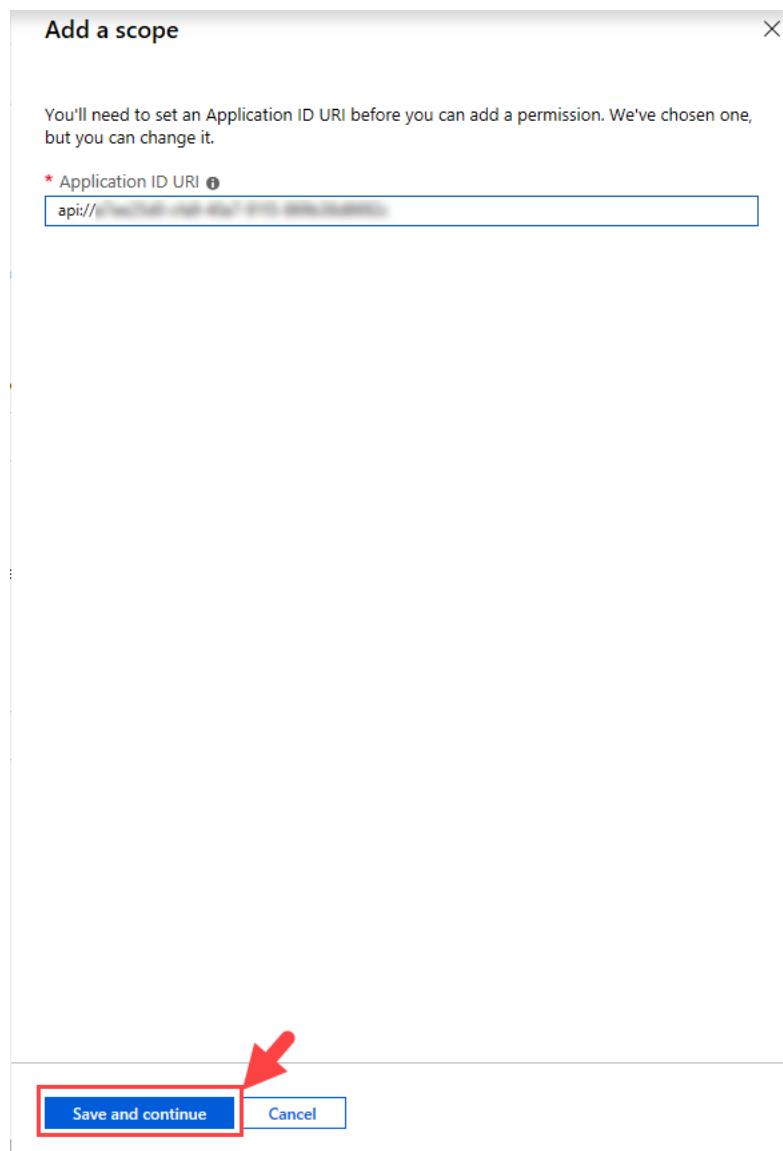
Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

CLIENT ID	SCOPES
No client applications have been authorized	

**Add a scope** window displays.



9. Accept the default value in the **Application ID URI** field and click **Save and continue**.  
The Scope definition page displays.

Add a scope

\* Scope name ⓘ  
user\_impersonation ✓  
api:// /user\_impersonation

Who can consent? ⓘ  
 Admins and users  Admins only

\* Admin consent display name ⓘ  
Access the ERP Server ✓

\* Admin consent description ⓘ  
Allow the application to access the ERP Server. ✓

User consent display name ⓘ  
Access the ERP Server ✓

User consent description ⓘ  
Allow the application to access the ERP Server on your behalf.

State ⓘ  
 Enabled  Disabled

**Add scope** **Cancel**



- a. Enter a **Scope name**.



**Tip** This name is displayed to users when they accept permissions during login. Suggested Scope name value is **user\_impersonation** but it can be anything meaningful to your company.

- b. In the **Who can consent?** toggle, select **Admins and users**.
- c. Enter **Admin consent display name** and **Admin consent description** - for example, as showed on the above screenshot.
- d. Optionally, enter **User consent display name** and **User consent description**. Use the above screenshot as an example.
- e. For the **State**, select **Enabled**.
- f. Click **Add Scope**.

10. If **Epicor Web Access (EWA)** and **Epicor Data Discovery (EDD)** extensions are deployed, specify additional **Redirect URIs** to enable Azure AD authentication for these web applications. Click **Authentication**. In the **Redirect URIs** grid, enter the URIs as shown in the below table; be sure to keep URI formats as listed below.

Application Name	Type	Redirect URI (Reply URL)
<b>EDD</b>	Public client (mobile & desktop)	<a href="https://servername/appname/index.html">https://servername/appname/index.html</a>
<b>EWA</b>	Public client (mobile & desktop)	<a href="https://servername/appname/ice.ewa.sysloginazure.aspx">https://servername/appname/ice.ewa.sysloginazure.aspx</a>

### Example

**REDIRECT URI**

---

<https://server/erp102400/home>

---

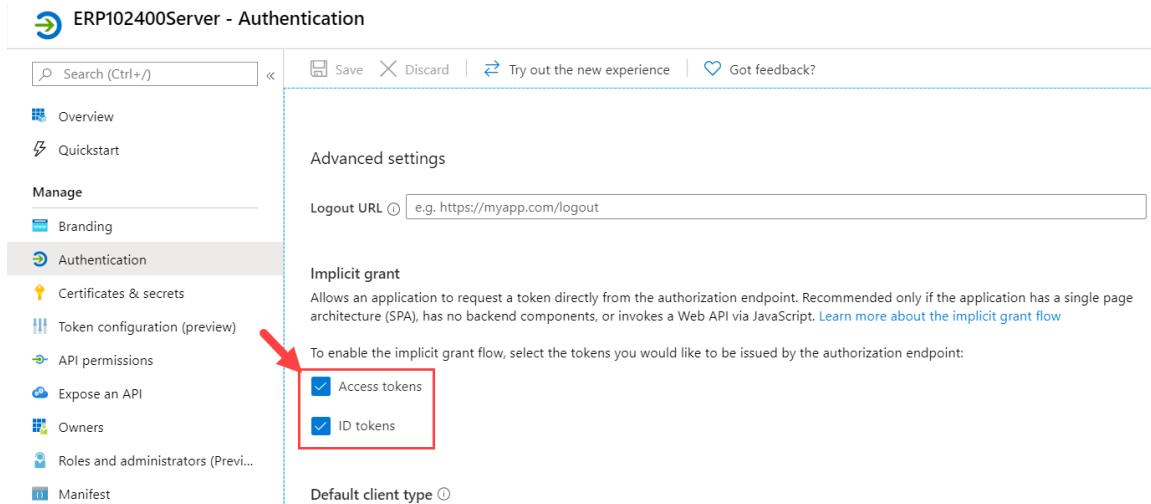
<https://server/erp102400-edd/index.html>

---

<https://server/erp102400-ewa/ice.ewa.sysloginazure.aspx>

**Important** Azure AD Redirect URIs are case-sensitive, be sure to use **lowercase** for these URIs as shown above. If needed, verify the exact extension URLs in the **Epicor Administration Console > Application Server Configuration > Extensions**.

11. Click **Authentication** to enable **Implicit grant** flow for Access tokens and ID tokens.



The screenshot shows the 'ERP102400Server - Authentication' page. On the left, there's a navigation menu with 'Overview', 'Quickstart', 'Manage' (selected), 'Branding', 'Authentication' (selected), 'Certificates & secrets', 'Token configuration (preview)', 'API permissions', 'Expose an API', 'Owners', 'Roles and administrators (Preview)', and 'Manifest'. The 'Authentication' section is expanded, showing 'Logout URL' (e.g. https://myapp.com/logout) and 'Implicit grant' settings. Under 'Implicit grant', it says: 'Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.' Below this, it says: 'To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:' with two checkboxes: 'Access tokens' and 'ID tokens', both of which are checked and highlighted with a red box. A red arrow points to this red box.

12. Select both **Access tokens** and **ID tokens** and **Save**.

**Note** Enabling **Implicit grant** automatically sets the **oauth2AllowImplicitFlow** Manifest setting to **true**.

## Register Client Application

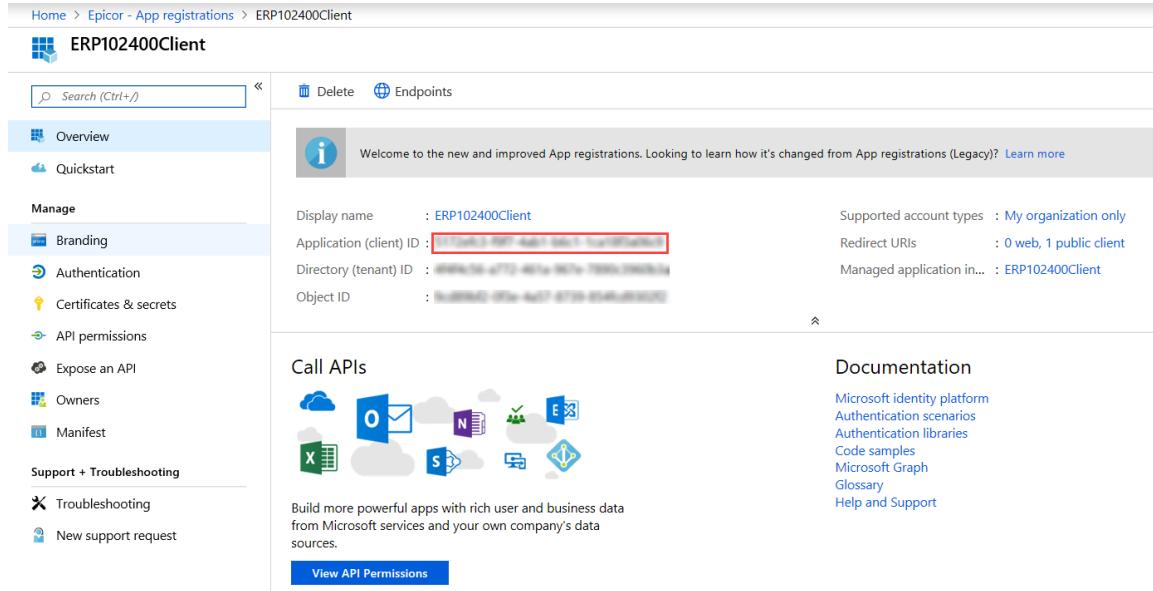
Now, create another application registration for **Epicor client**.

1. Click on **App registrations** and select **+ New registration**.
2. Enter a **Name**. You may use the format of <ApplicationName> + Client - for example, **ERP102x00Client**.
3. Keep the default option in the **Supported account types** section.
4. From the **Redirect URI** type drop-down, select **Public client/native (mobile & desktop)**. For the URI, Epicor recommends using **https://localhost**.

 **Note** This URI is verified during the logon process and does not need to point to any specific location. If, for any reason, this default value needs to be changed, new URI must be specified in application's sysconfig optional setting **<AzureADRedirectUri value="" />**.

## 5. Register the application.

The application overview page displays.



The screenshot shows the Azure App Registrations overview page for the application 'ERP102400Client'. The left sidebar includes links for Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets, API permissions, Expose an API, Owners, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area displays the application details:

Display name	: ERP102400Client	Supported account types	: My organization only
Application (client) ID	(highlighted with a red box)	Redirect URLs	: 0 web, 1 public client
Directory (tenant) ID	: A999A999-A999-A999-A999-A999A999A999	Managed application in...	: ERP102400Client
Object ID	: BBBBBBBB-BBBB-BBBB-BBBB-BBBBBBBB BBBB		

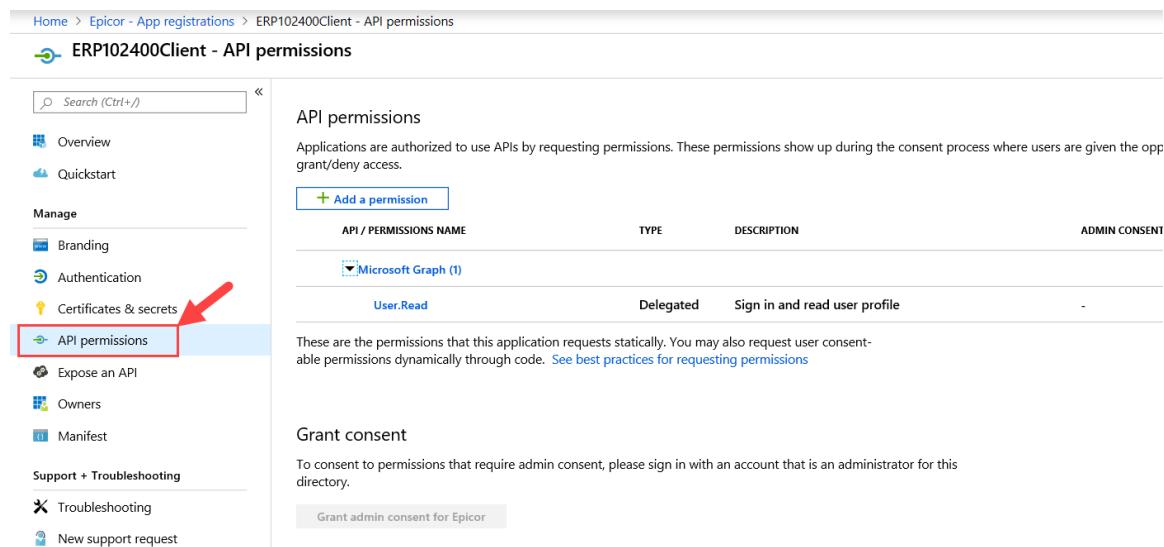
Below the details, there are sections for 'Call APIs' (with icons for various Microsoft services like SharePoint, OneDrive, etc.) and 'Documentation' (links to Microsoft identity platform, authentication scenarios, libraries, samples, Graph, Glossary, and Help and Support). A note at the bottom says 'Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.' and a 'View API Permissions' button.

Take note of the **Application (client) ID** value. You enter this value into the **Native Client Application ID** field of the **Azure Active Directory Settings Maintenance** program. In the Epicor ERP application's sysconfig, this value needs to be specified in the **AzureADNativeClientAppID** setting.



**Example** `<AzureADNativeClientAppID value="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx" />`

6. Now, specify that this application is going to connect to the Epicor server application. In the **Manage** panel on the left side of the screen, click **API Permissions**.



The screenshot shows the 'API permissions' page for the 'ERP102400Client' application. The left sidebar includes links for Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets, API permissions), Expose an API, Owners, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The 'API permissions' link is highlighted with a red box and an arrow. The main content area displays the 'API permissions' section, which lists a single permission: 'User.Read' under 'Microsoft Graph (1)'. The permission is of type 'Delegated' and describes 'Sign in and read user profile'. Below this, a note states: 'These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. See best practices for requesting permissions'.

 **Tip** To get to the API Permissions page, you can also click **View API Permissions** in the **Call APIs** section of the application overview page.

## Call APIs



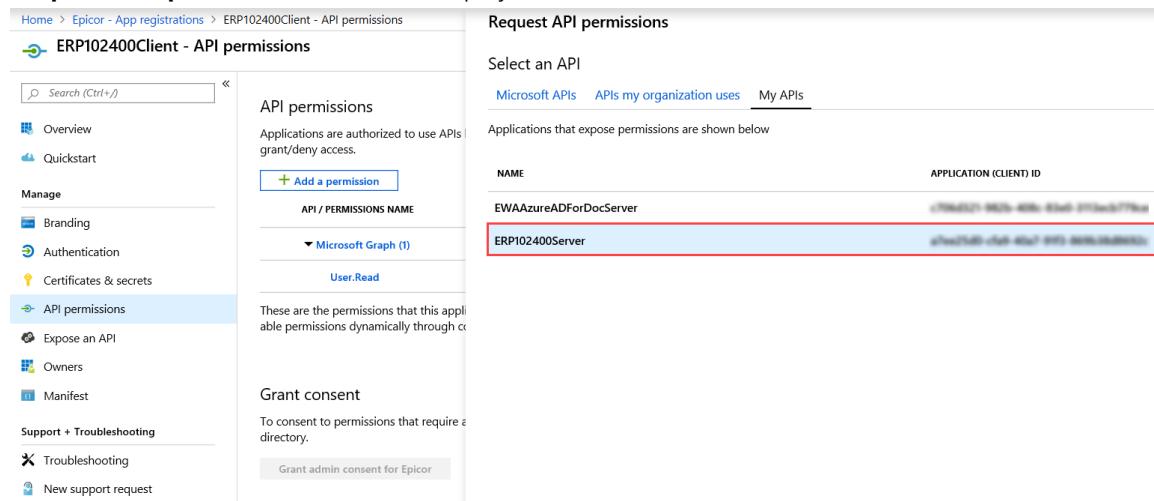
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

**View API Permissions**

The **API Permissions** page displays.

### 7. Click **Add a permission**.

The **Request API permissions** window displays.



The screenshot shows the 'Request API permissions' window. It has tabs for 'Microsoft APIs', 'APIs my organization uses', and 'My APIs'. The 'APIs my organization uses' tab is selected, showing a table with two rows: 'EWAAzureADForDocServer' and 'ERP102400Server'. The 'ERP102400Server' row is highlighted with a red box and an arrow. The left sidebar of the window is identical to the one in the previous screenshot, showing links for Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets, API permissions), Expose an API, Owners, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The 'API permissions' link is also highlighted with a red box and an arrow.

### 8. Select the previously created server application from the **APIs my organization uses** or **My APIs** tab.

**9.** Select the permission and click **Add permissions**.

The screenshot shows the 'Request API permissions' dialog. At the top, it says 'ERP102400Server' and 'api://[REDACTED]'. Below that, it asks 'What type of permissions does your application require?' with two options: 'Delegated permissions' (selected) and 'Application permissions'. Under 'Delegated permissions', it says 'Your application needs to access the API as the signed-in user.' Under 'Application permissions', it says 'Your application runs as a background service or daemon without a signed-in user.' A large table follows, titled 'Select permissions' with columns 'PERMISSION', 'ADMIN CONSENT REQUIRED', and a search bar 'Type to search'. One row is shown: 'user\_impersonation' (checked), 'Access the ERP Server', and '-' under Admin Consent Required. A red arrow points to the 'Add permissions' button at the bottom left of the table.

PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access the ERP Server ⓘ	-

The new permission is added to the list on the **API permissions** page.

The screenshot shows the 'API permissions' page. It has a warning banner: 'Permissions have changed. Users and/or admins will have to consent even if they have already done so previously.' Below is a table with columns 'API / PERMISSIONS NAME', 'TYPE', 'DESCRIPTION', and 'ADMIN CONSENT REQUIRED'. A red box highlights the entire table. One row is visible: 'ERP102400Server (1)' expanded to show 'user\_impersonation' (Delegated, Access the ERP Server, Admin Consent Required: -).

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
ERP102400Server (1)			
user_impersonation	Delegated	Access the ERP Server	-

**10.** You may review created permission by clicking **Manifest** in the left-side **Manage** panel.

```

41     },
42   ],
43   "requiredResourceAccess": [
44     {
45       "resourceAppId": "a1f60000-0000-4000-9000-000000000000",
46       "resourceAccess": [
47         {
48           "id": "a1f60000-0000-4000-9000-000000000000",
49           "type": "Scope"
50         }
51     ],
52     {
53       "resourceAppId": "a1f60000-0000-4000-9000-000000000000",
54       "resourceAccess": [
55         {
56           "id": "a1f60000-0000-4000-9000-000000000000",
57           "type": "Scope"
58         }
59     ]
60   ],
61   "samlMetadataUrl": null,
62   "signInUrl": null,
63   "signInAudience": "AzureADMyOrg",
64   "tags": [],
65   "tokenEncryptionKeyId": null
66 },
67 ],
68 }

```

Notice the first **resourceAppId** is equal to the Application ID of the server application.

## Epicor Administration Console Bindings

Deploy the application server using binding(s) created specifically for communication with Azure Active Directory. You configure these properties in the Epicor Administration Console.

1. On your server, launch the **Epicor Administration Console**.
2. Use the tree view to navigate to the application server. Expand the **Server Management** node, and then the **<ServerName>** node. The application server(s) display.
3. From the **Actions** pane, click **Application Server Configuration**.
4. Specify Endpoint Bindings:
  - **Net.Tcp Endpoint Binding** - Determine your authentication option based on your company's best practice method for security.
  - **Http Endpoint Binding** - Determine your authentication option based on your company's best practice method for security.

For scenarios when encryption handling to an intermediary Application Request Router like F5 or a similar router is implemented, select the **HttpsOffloadBinaryAzureChannel** option.

  - **Https Endpoint Binding** - select the **HttpsBinaryAzureChannel** option.



**Important** To enable integration with DocStar, you will need to set up another Epicor ERP application server that will be connected to the same ERP database, because both Azure AD and DocStar require Https Endpoint Binding to connect to ERP. Please contact **Epicor Integration Team** for details.

## 5. Deploy the application server. Once complete, click **OK**.

You may verify the selected bindings are written to the application's web.config file in the <protocolMapping> section. For example:

```
<protocolMapping>
    .....
    <remove scheme="http" />
    <add scheme="http" binding="customBinding" bindingConfiguration="Http
soffloadBinaryAzureChannel" />
    <remove scheme="https" />
    <add scheme="https" binding="customBinding" bindingConfiguration="Htt
psBinaryAzureChannel" />
</protocolMapping>
```

## Configure Azure AD Authentication

You now configure authentication settings between the Epicor ERP application and Azure Active Directory.

Log into Epicor ERP and navigate **Azure Active Directory Configuration Maintenance**.

**Menu Path:** System Setup > Security Maintenance > Azure Active Directory Settings

### 1. Click **New**.



**Note** Azure Active Directory ID and Web Application ID fields are mandatory for each configuration.

### 2. Enter your company's **Azure Active Directory ID** (Tenant ID). To obtain this value:

- a. Log on to the Microsoft® Azure® portal <https://portal.azure.com>.
- b. In the left navigation panel, select **Azure Active Directory**.
- c. Click on **Properties** and take note of **Directory ID** value.

### 3. Enter your Epicor Server **Web Application ID**. This values serves as an audience in the security access token. To obtain this value:

- a. Log on to the Microsoft® Azure® portal <https://portal.azure.com>.
- b. In the left navigation panel, select **Azure Active Directory**.
- c. Click on **App registrations**.
- d. Select the Epicor Server web application and take note of the **Application ID** value.

The remainder of the fields is optional.

### 4. Enter a concise **Description** for this Azure Active Directory configuration.

### 5. You may use **Authentication Claim** field to change the default security token (authentication claim), used to create a mapping between an Epicor ERP 10 user and Azure Active Directory user.

The security token issued by AAD contains various types of claims that may be used for authentication. The list of available claims includes:

- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name` - **default claim**; corresponds to `unique_name` claim within the token. For example:  
`"unique_name" : "sample.user@contoso.onmicrosoft.com"`,
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` - corresponds to email claim within the token. For example:  
`"email" : "frankm@hotmail.com"`,

 **Note** In most cases, usage of the default claim should work and there is no need to specify any value in this field. You may, however, specify any supported Azure AD claim in this field. You then need to properly specify **External Identity** of a user so it matches the authentication claim. You specify External Identity in the **User Account Security Maintenance**.

Also, if you specify a claim other than default, but it is not found in the security token issued by Azure AD, the default claim is used instead.

 **Tip** For more information on tokens claims, see the [Microsoft® Azure® documentation](#).

**6.** Enter the **Native Client Application ID**. To obtain this value:

- a. Log on to the Microsoft® Azure® portal <https://portal.azure.com>.
- b. In the left navigation panel, select **Azure Active Directory**.
- c. Click on **App registrations**.
- d. Select the Epicor native application and take note of the **Application ID** value.

**7.** Select the **Use as Default Configuration** checkbox to indicate the current configuration settings may be promoted to clients' sysconfig files.

 **Important** You can create multiple AAD configuration settings on this form, however, one of them needs to be marked as default.

When a user logs in, the application first verifies if **AzureADNativeClientAppID** property (Native Client Application ID) is specified in the client's sysconfig file. When missing, the application checks if there is at least one Azure AD configuration record with this check box is enabled. If multiple configurations are set as default, the first one on the list is used. The client's sysconfig is then updated with Azure Directory ID, Web application ID and Native application ID.

SaaS customers are first presented with the dialog where they need to enter their 6-digit Epicor Tenant ID.

**8. Save** the record and exit the application.

## Update User File

Use the User Account Security Maintenance form to create mapping between an Epicor ERP 10 user and a user in Azure Active Directory.

**1. Navigate to User Account Security Maintenance.**

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

2. Retrieve a record for a user.

3. Now specify **External Identity** for this user.

A typical entry for an external identity would be a valid email address.



**Note** A value in this field needs to correspond to a claim specified in **Azure Active Directory Configuration Maintenance > Authentication Claim** field.

4. **Save** the record.

## Update Client .sysconfig

This topic discusses mandatory and optional configuration settings for a client installation's .sysconfig file.

1. Update the application server URL so it uses the **https** scheme, for example:

```
<AppServerURL value="https://<AppServerName>/ERP102200" />
```

2. Set the **EndpointBinding** value to **HttpsBinaryAzureChannel**.

```
<EndpointBinding value="HttpsBinaryAzureChannel" options="...." />
```

3. The below three values must be supplied for each client.



**Note**

- You may update these properties manually.
- You can have the application update these settings automatically on the first logon. This approach assumes these values are filled in Azure Active Directory Configuration Maintenance and the configuration is marked as default.

Property	Description
<AzureADDirectoryID value=" " />	Enter Azure Tenant ID (Directory ID) from Azure AD Properties.
<AzureADWebApplID value=" " />	Enter Azure AD Web Application ID of a registered Server application.
<AzureADNativeClientApplID value=" " />	Enter Azure AD Native Client Application ID of registered native application.



**Tip** See **Configure Azure Portal** and **Configure Azure AD Authentication** topics, if needed.

4. The below table lists optional settings for each client:

Property	Description
<AzureADInstance value=" " />	Use this property to specify a template for logon URL other than default: https://login.microsoftonline.com/{0}
<AzureADRedirectUri value=" " />	If other location than default (https://localhost) is used as Redirect URI in a native client application, use this property to specify that URI in .sysconfig for each client. For more information, see the <b>Configure Azure Portal</b> topic.

## Update .sysconfig on Logon

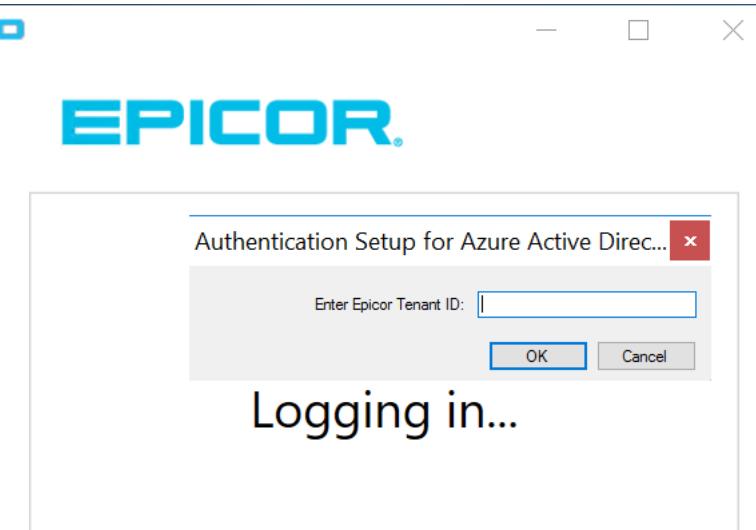
This topic explains how to update client's sysconfig on the first logon with Azure Active Directory (AAD) settings, if they are not yet specified.

1. When a user logs into ERP 10, the application first verifies if **AzureADNativeClientAppID** property (Native Client Application ID) is specified in the client's sysconfig.
2. When missing, the application checks if there is at least one AAD configuration with **Use as Default Configuration** property enabled in **Azure Active Directory Configuration Maintenance** form.



**Note** If more than one configuration is marked as default, the first one on the list is used.

3. SaaS customers are presented with the following dialog, where they need to enter their 6-digit Epicor Tenant ID. This dialog does not display for on-premise customers.



4. If a valid configuration is found, it is written into the client's .sysconfig and the logon process continues.



**Tip** If you need, you may verify the REST .configuration page by using the following URLs:

- On-premise install: [https://\[MyAppServerHost\]/\[MyAppServerInstance\]/api/.configuration?TenantID=<tenant\\_id>](https://[MyAppServerHost]/[MyAppServerInstance]/api/.configuration?TenantID=<tenant_id>)
- SaaS install: [https://\[MyAppServerHost\]/\[MyAppServerInstance\]/api/.configuration?TenantID=<Epicor Tenant ID>](https://[MyAppServerHost]/[MyAppServerInstance]/api/.configuration?TenantID=<Epicor Tenant ID>)

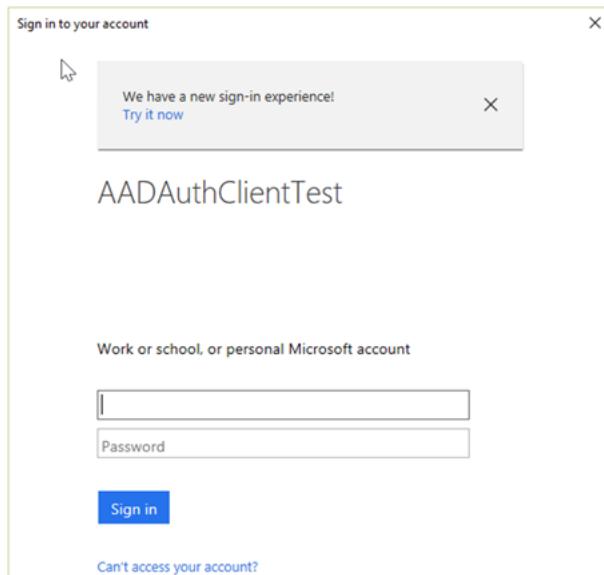
The following is an example of an on-premise configuration:

```
{  
    "TokenAuthentication": {  
        "Enabled": true,  
        "UsesWindowsBinding": false  
    },  
    "AzureADSettings": {  
        "DirectoryID": "xxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  
        "WebAppID": "xxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  
        "NativeClientAppID": "xxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  
        "Description": "Azure AD Configuration"  
    }  
}
```

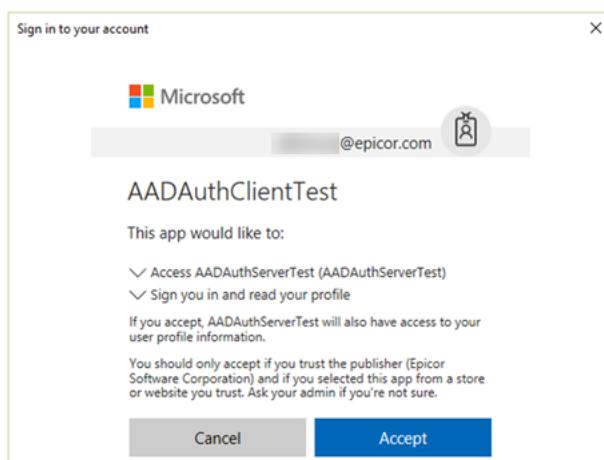
## Login Process

You are now ready log into Epicor ERP using Azure AD authentication.

1. When you launch the client for the first time, you are presented with the Microsoft® logon page.



2. Enter your Azure AD login credentials and click **Sign in**.
3. Click **Accept** on the dialogs that follow.



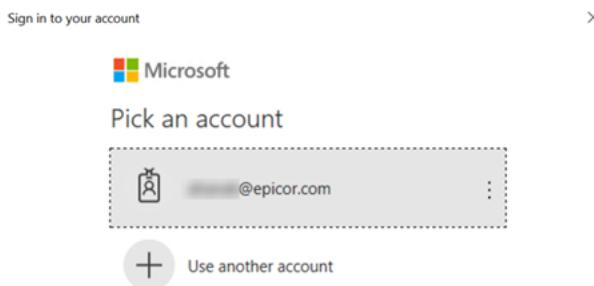
At this stage, the client obtains the security token issued by Azure AD and user logs into the Epicor ERP application.



**Note** Security Token is cached after the first use and saved as encrypted into the AppData subdirectory:  
C:\Users\<User>\AppData\Roaming\epicor\AzureAD\<Version>\<AzureADWebAppID>\<AzureADNativeClientApp>

Token is usually valid for several hours; when it expires, it is automatically retrieved by the application.

4. Next time you log in, you are presented with the previously used Azure AD identity.



## Optional Server Settings

Standard Nuget library Microsoft.IdentityModel.Protocols.dll is used to work with Azure AD key management. Key manager classes are cached; key values are refreshed periodically, by default once a day.

Azure AD key management on server does not require any mandatory setting. The below table lists optional settings that may be configured within the appSettings section of an application server's web.config file.

Property	Description
<AzureADInstance value=" " />	Use this property to specify a template for logon URL other than default: <code>https://login.microsoftonline.com/{0}</code> <code>&lt;add key="AzureADInstance" value="https://login.microsoftonline.com/{0}" /&gt;</code>
<AzureADDDiscoveryEndPointSuffix" value=" " />	Suffix for the discovery URL. Default value is .well-known/openid-configuration: <code>&lt;add key="AzureADDDiscoveryEndPointSuffix" value=".well-known/openid-configuration" /&gt;</code>
<AzureADKeyAutomaticRefreshInterval" value="0" />	Timespan setting to specify how often keys will be re-read from Azure. Default value is once in 24 hours. Minimum possible value is 5 minutes. For example: <code>&lt;add key="AzureADKeyAutomaticRefreshInterval" value="2.00:00:00" /&gt;</code>
<AzureADKeyRefreshInterval" value=" " />	The minimum time between retrievals, in the event that a retrieval failed, or that a refresh was explicitly requested. Default value is 30 seconds. Minimum value is 1 second. For example: <code>&lt;add key="AzureADKeyRefreshInterval" value="00:00:10" /&gt;</code>

## Multi-Factor Authentication via Azure AD

Azure Active Directory supports the ability to use multi-factor authentication, with a range of easy verification options, such as phone call, text message, or mobile app notification.

There are additional authentication options which may be implemented by customers using higher versions of Azure AD (Premium1 and Premium P2 editions), such as Identity Protection, end-user self-service or Policy Driven Access.

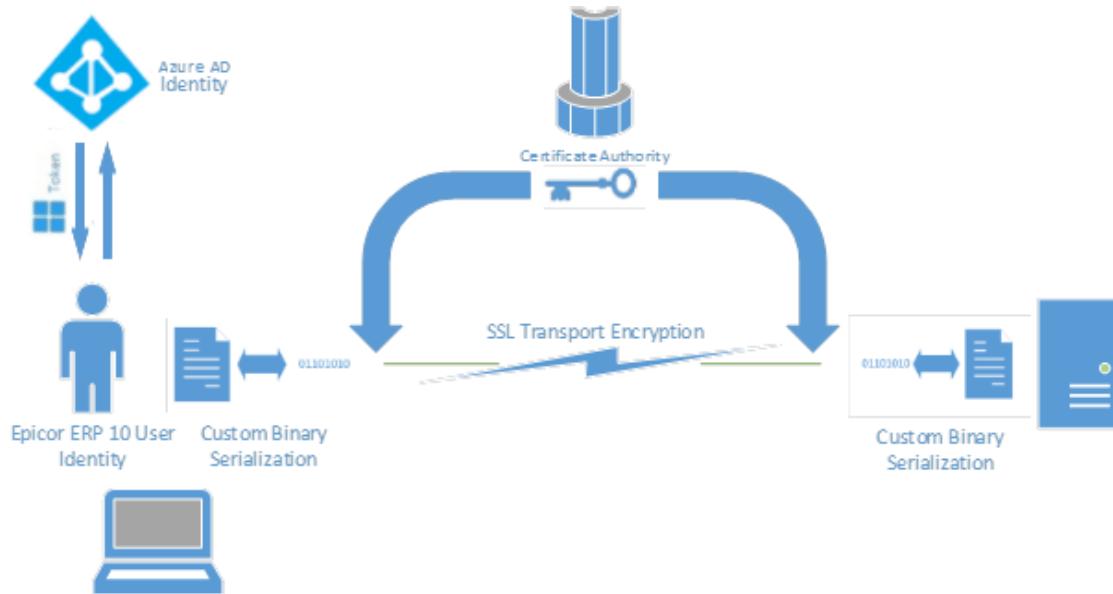
For more information, Epicor recommends reviewing of the below Microsoft® Azure® sources:

- **Multi-Factor Authentication Introduction:** <https://azure.microsoft.com/en-us/services/multi-factor-authentication/>
- **Multi-Factor Authentication Documentation:** <https://docs.microsoft.com/en-us/azure/multi-factor-authentication/>
- **Multi-Factor Authentication Overview:** <https://channel9.msdn.com/Blogs/Azure/WA-MFA-Overview>

## Troubleshooting

This section explains how to activate server and client logging in order to troubleshoot Azure AD authentication problems. It also provides answers to common authentication errors users may experience.

The following diagram illustrates how HttpsBinaryAzureChannel binding handles network transactions. This scenario assumes your company uses Azure Active Directory as an authentication provider for applications.



- User logs in against Azure AD: Office 365 Outlook, Yammer, etc.
- Azure AD provides the client a security token.
- Client sends token to server on each call.
- Server verifies the token against Azure.

## Client Logging

You may activate the client log to see all exceptions caught during the logon process.

To turn on logging, uncomment the `<add name="DataTrace" value="4" />` switch found in

```
<system.diagnostics>
  <switches>
```

section of Epicor.exe.config (Epicor64.exe.config) file found in ERP 10 client directory.

In addition, by activating the client logging, **Azure Active Directory Authentication Library (ADAL) log** file gets created in `C:\Users\<User>\AppData\Roaming\epicor\AzureAD\<Version>\<AzureADWebAppID>\<AzureADNativeClientAppID>\` folder.

## Server Logging

Use the server log if you need to obtain detailed information about the Azure Active Directory authentication process.

In order to log the authentication process, activate server logs from within the Epicor Administration Console and enable the following trace flag in AppServer.config:

- <add uri="profile://system/security" />

 **Tip** For detailed information on how to use server logs, see the **Performance Tuning Guide > Customize Logs > Server Log Customization** topics.

## Solving Logon Errors

This topic covers several example errors caught while logging into Azure AD along with their resolution.

-  **Example** An error occurred when verifying security for the message.

```
Error Detail  
=====  
Message: An error occurred when verifying security for the message.  
Program: CommonLanguageRuntimeLibrary  
Method: HandleReturnMessage
```

**Resolution:** Https binding is set incorrectly in web.config; verify the line <add scheme="https" binding="customBinding" bindingConfiguration="HttpsBinaryAzureChannel" /> is present.

-  **Example** Resource permission problem.

```
Exception Caught in Microsoft.IdentityModel.Clients.ActiveDirectory  
Error Detail  
=====  
Message: Invalid Resource. The client has requested access to a resource  
which is not listed in the requested permission in the client's applica  
tion registration.  
Program: Microsoft.IdentityModel.Clients.ActiveDirectory  
Method: VerifyAuthorizationResult
```

**Resolution:** Permissions are not configured for the client app registration. See the **Azure AD Authentication > Configure Azure Portal** topic, steps **5.g) - 5.j)**.

-  **Example** Proxy related error.

```
Exception Caught in Microsoft.IdentityModel.Clients.ActiveDirectory  
Error Detail  
=====  
Message: The browser based authentication dialog failed to complete. Rea  
son: The server or proxy was not found.  
Program: Microsoft.IdentityModel.Clients.ActiveDirectory  
Method: ShowBrowser
```

**Resolution:** Client machine cannot connect to either Azure AD URL: <https://login.microsoftonline.com>, or, when using federation, the client machine cannot connect to a federation endpoint, such as <https://sts.yourcompany.com> or <https://sso.yourcompany.com>. Please contact your company IT administrator.

-  **Example** Audience validation failed.

```
Exception Caught in Epicor.ServiceModel  
Error Detail  
=====  
Message: IDX10231: Audience validation failed. Delegate returned false,
```

```
securitytoken {...}...
Program: Epicor.ServiceModel.dll
Method: ShouldRethrowNonRetryableException
```

**Resolution:** In Epicor ERP 10, the Azure Active Directory Settings form is missing the settings for Directory ID and Web Application ID.

-  **Example** User is not setup for external provider sign-on

```
Exception caught in: mscorlib
Error Detail
=====
Message: <User> is not setup for external provider sign-on.
Program: CommonLanguageRuntimeLibrary
Method: HandleReturnMessage
```

**Resolution:** No mapping is added to the User Account Security Maintenance for this Azure user, so no Epicor user could be mapped with the identity email provided.

For more information on how to create mapping between an Epicor ERP 10 user and a user in Azure Active Directory, see the [Azure AD Authentication > Update User File](#) topic.

## Epicor Identity

Epicor Identity Provider (IdP) is an authentication service that unifies various identity and authentication mechanisms across Epicor products, ensuring secure and easy to use products.

The following is the list of key IdP features:

- centralized identity management,
- multi-factor authentication,
- bridge to other authentication mechanism and providers,
- user account self-service,
- automated user provisioning and deprovisioning.

 **Important** As of Epicor **ERP 10.2.700**, Epicor **ERP Cloud** customers may opt in using IdP authentication

The following is the high-level flow of operations:

- ERP Cloud customer creates a request in EpicCare to leverage IdP authentication for a tenant.
- The registration process requires a new Tenant Application Administrator email address. Epicor recommends using at least two Application Administrator roles per tenancy.
- Registration email is sent by IdP Administrator or IT support to a Tenant Application Administrator(s).
- Application Administrator adds/invites/maps users to Identity Provider.
- Application Administrator configures Identity Provider settings, such as Multi-factor authentication, Password policy, allowed External providers and so on.
- All user workstations using IdP authentication must have access to the internet.

Note this feature is **not available for on-prem customers**.

As of writing this guide, a single global login may be used to gain access to the following Epicor products using IdP:

- Epicor ERP
- Epicor Learning Center
- Epicor Docstar
- EpicCare



## Authentication Overview

Epicor Identity Provider allows applications to authenticate users registered in the common user database. Epicor Identity Provider issues signed tokens, which contain claims with required information. These tokens can be validated using Epicor Identity Provider public key. This topic describes relations between tokens, claims and resources in Epicor Identity Provider.

### Tokens

Epicor Identity Provider uses two types of JWT tokens:

- Identity Token (id token) - represents the outcome of an authentication process. It contains at a bare minimum an identifier for the user (called subject claim) and information about how and when the user authenticated. It may also contain additional identity data. Identity tokens are used on the UI client side.
- Access Token - sent to the server to allow access to an API resource. Clients request access tokens and forward them to the API. Access tokens contain information about the client and the user (if present). APIs use that information to authorize access to their data.

JWT token contains signed encoded information for authentication in JSON format. The following is an access token example:

```
eyJhbGciOiJSUzI1NiIsp0tpZCI6ImVhNTdhNWJ1ODVhNWFim2NjZWY4ZjdkODJmN2FjZjk1IiwidHlwIjoisldUIIn0.
eyJJuYmYiOjE1NjIyNzY2OTIsImV4cCI6MTU2MjI4MDI5MiwiaXNzIjoiaHR0cHM6Ly9sb2NhbgvC3Q6NDQzMjgvDGlkL2E
wMDAwMDAwLTAwMDAtMDAwMC0wMDAwLTAwMDAwMDAwMCIsImF1ZCI6WyJodHRwczovL2xvY2FsaG9zdDo0NDMyOC90aW
QvYTAwMDAwMDAtMDAwMC0wMDAwLTAwMDAtMDAwMDAwMDAwL3Jlc291cmNlcycIsImVwaWNvc191cnAiXSwiY2xpZW50X
21kIjojNDR1MThjY2YtOGU4MS00NDZiLTgwOWQtNzI0YzhmNTY2MGVjIiwic3ViIjoiYWY3OTFlMGUTNmFlyi00MDAxLWJk
OGEtMDhkNjFlNTFiMjk5IiwiYXV0af90aW11IjoxNTYyMjczNzk3LCJpZHAIoIJsB2NhbCIsImVtYw1sIjoib2tsaW1vdmF
AZXBpY29yLmNvbSIsInNjb3BlIjpbIm9wZW5pZCIsImVtYwlsIiwiZXBy29yX2VycCJdLCJhbXIiOl
sicHdkI119.Cs0yL
dPO3kxmc0hUq2GJ--8bwLfbRKyhu_nWofoygEgg5F7EdEda5YnH8xaJaF9pla8vzAnupSUU-7xby88izKjIp
mx_cmg35Xa7
UvoBTGAbSQsn7HPRQ175Hy3YeNQmjzo2Y0vDAJixrQTtxjVpse-sFwkOisVKTUVaUkzJX1oUormvgwmLRfatf4uIkTXNB0
pD4-UfRUVmvwgsVVJpk8i3k14dtodif3LD08oMdgc75irTdxUw9ETt_Vx2JIocnn7nPCqSKNL_yX0VA
TOOLkEq1a4C_b5i1
PB_6amtstCcsqfVsfeevKPWyyoDOKTyW7BScoLiyxgB_-06bXj3tg
```

You can review the content of access (or any JWT) token by pasting it in the forms using either <https://jwt.ms/> or <https://jwt.io/>.

```
{
  "alg": "RS256",
  "kid": "ea57a5be85a5ab3cce8f7d82f7acf95",
  "typ": "JWT"
}.{
  "nbf": 1562276692,
  "exp": 1562280292,
  "iss": "https://idp.developer.epicor.com/tid/a0000000-0000-0000-0000-000000000000",
  "aud": [
    "https://idp.developer.epicor.com/tid/a0000000-0000-0000-0000-000000000000/resources",
    "epicor_erp"
  ],
  "client_id": "44e18ccf-8e81-446b-809d-724c8f5660ec",
  "sub": "af791e0e-6aeb-4001-bd8a-08d61e51b299",
  "auth_time": 1562273797,
  "idp": "local",
  "email": "user@epicor.com",
  "scope": [
    "openid",
    "email",
    "epicor_erp"
  ],
  "amr": [
    "pwd"
  ]
}.[Signature]
```

The following highlights technical details of how Epicor ERP server validates token:

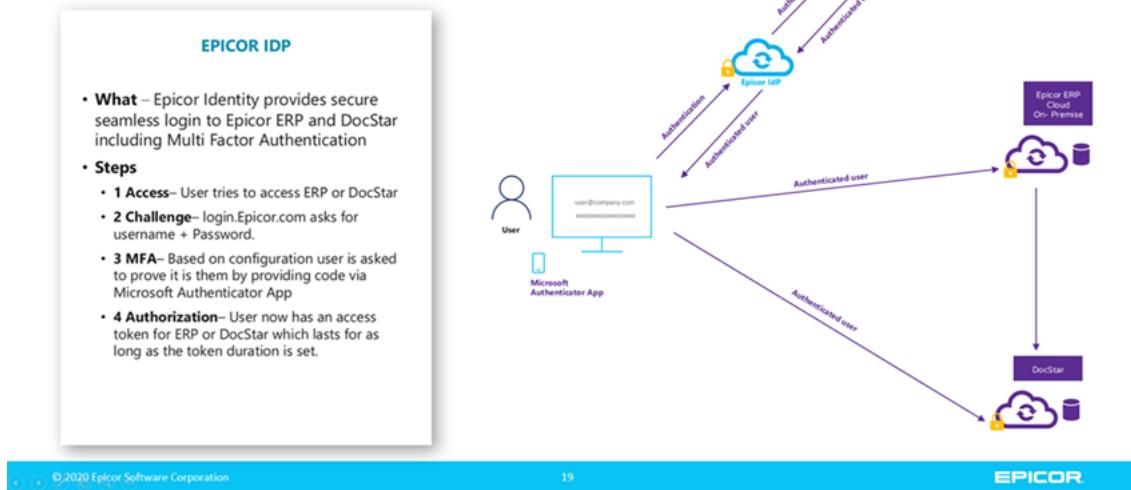
- Epicor ERP validates the access token via JWT validation (including signature validation), following the same validation process implemented for Azure AD access tokens.
- When an access token is received by an API server, such as Epicor ERP, the signature of the token is always checked by the server using the kid (key identifier) claim from the token header and verifying that it matches the public key provided by an Epicor Identity Provider server. To retrieve the key, the API server uses the .well-known/openid-configuration endpoint for Identity Provider's tenant. Common configuration for all tenants looks as follows: <https://idp.developer.epicor.com/.well-known/openid-configuration>.

This endpoint contains the jwks\_uri item, that points to the public key(s) to verify token. For example: <https://idp.developer.epicor.com/tid/a0000000-0000-0000-000000000000/.well-known/openid-configuration/jwks> contains kid: ea57a5be85a5ab3cce8f7d82f7acf9. If the token header contains this kid value, the token integrity can be verified. If the key is not found, an error is returned by the API server.

- On each call, an API server also verifies the following mandatory claims:
  - **iss** - issuer, URL of the Epicor Identity Provider, for example, https://idp.developer.epicor.com, with tenant-specific suffix: **/tid/<tenantId>**.
  - **aud** - audience, name of API resource in Epicor Identity Provider.
  - **exp** - expiration time of the token.
  - **scope** - scope of the token, one or more scopes from the Epicor Identity Provider API resource.

If either of the claims does not correspond to a value predefined in API server, or if the token life-time is expired, authentication fails.

# Epicor Identity



## Claims

Besides mandatory claims mentioned above, a token may contain additional claims required by an API server. For example, Epicor ERP requires **email** claim to be included in the token to map Epicor Identity Provider user to an internal Epicor user, such as manager. The list of claims that may be added to the token are defined in Epicor Identity Provider resources. For access tokens, claims should be specified in the API resource (or in one of its scopes requested during the token creation). For id tokens, claims are specified in the Identity resource. When tokens are requested during authentication, developer specifies scope(s), requested from Epicor Identity Provider. Claims for those scopes (or for parent API resource) are added to the tokens.

## Resources

Epicor Identity Provider defines two types of the resources:

- **Identity resource** - resource to define id token. The name of the resource is the name of the scope.
- **API resource** - resource to define access token. It contains one or more scopes.

Names of the scopes are globally unique in the system. When the client code requests one or more scopes, related resources are retrieved. Each resource or scope can define the list of the claims to be added to the token. These claims are taken from the current user and added to the token being created. Claims from identity resource are added to the identity token. Claims from API resource or scope are added to the access token.

## Obtaining a Token

This topic highlights the process of obtaining a token.

- Client Authenticates to Epicor IdP and is provided with different options based on configuration (Local client, Azure AD, Google ID, Certificate ...).
- Upon successful authentication, the server redirects to a client callback point with the Token (a landing page URL).



As of writing this guide, the following is the list of default claims supported by Epicor IdP. Additional claims may be supported in later versions of Epicor ERP.

Claim	Description
sub	Subject name. In Epicor IdP, this value refers to UserID GUID PK.
name	User name. In Epicor IdP, this value is always an email address.
email	User's email address.
preferred_username	User's email address.
role	One or more roles assigned to user in E IdP, such as Security Manager.
email_verified	True or False.
phone_number	User's phone number.
phone_number_verified	True or False.
tid	Current tenant ID.
given_name	User's first name.
family_name	User's last name.
auth_time	Time of authentication.



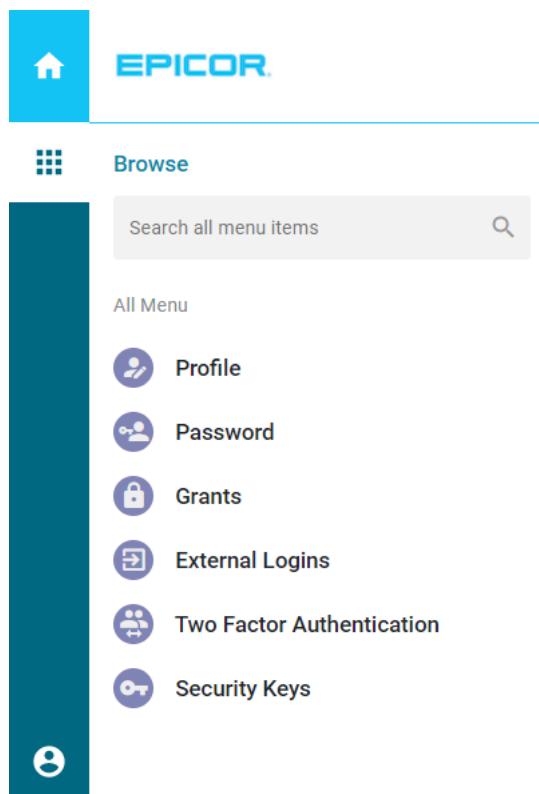
**Note** Presence of the above claims in tokens is based on a selected resource or scope definition.

## Account Self-Service

Epicor IdP users may use the My Account self-service page to manage and update their account settings.

The list of available controls includes:

- **Profile** - manage identity information such as Name, Phone number and so on.
- **Password** - reset IdP password following the password policy defined for a tenancy.
- **Grants** - displays the applications a user was given access to and the resources each application uses.
- **External Logins** - associate IdP account with external login provider(s) configured in a tenancy.
- **Two Factor Authentication** - enable Two-factor authentication for an account, configure Authenticator application, generate recovery codes.
- **Security Keys** - add Security Key(s) for Passwordless authentication using devices such as YubiKey, USB token, smart phone fingerprint or Windows Hello.



## Multi-factor authentication

Epicor IdP enables using additional layer of security to verify user's identity by requiring them to present more than a user name and password.

Typically, Application Administrator controls MFA availability for a tenant in Epicor IDP Administration page on the Multi-factor authentication card.

The following is the list of available MFA options:

- **Enabled** - default option, allowing users decide whether to use additional security check.
- **Disabled** - prevents using MFA method in the tenant.
- **Required** - enforces additional security check for users on logon. Users are not allowed to disable Two-Factor Authentication, when MFA is Required

The following are the available MFA options:

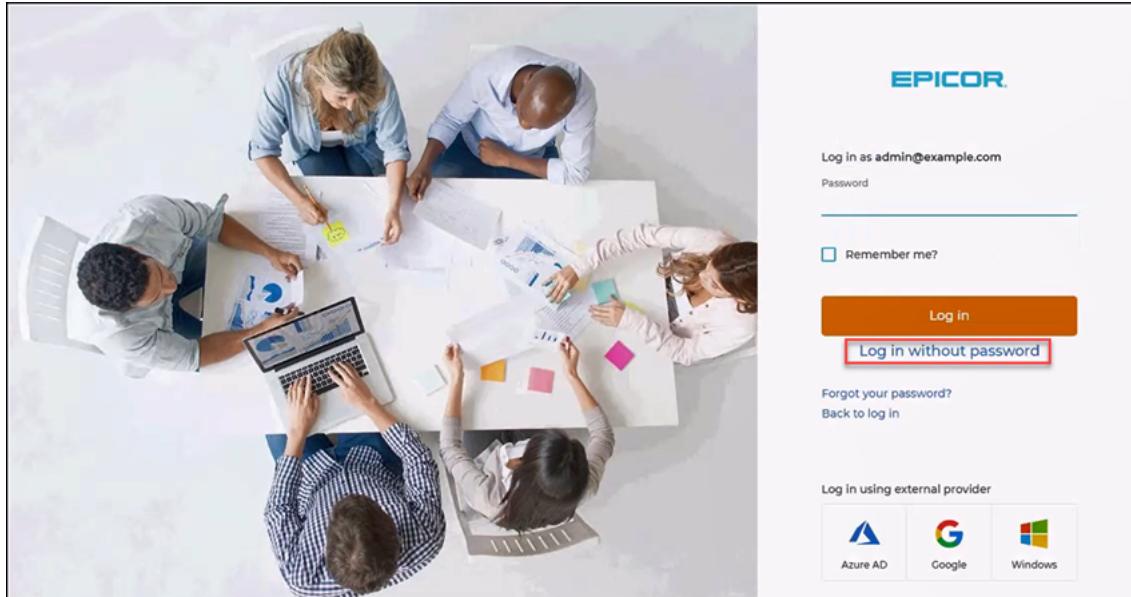
- **One-time password** - with this option selected, users authenticate by entering One-time access code during the logon using either of the below approaches:
  - **Via email** - One time verification code valid for 30 seconds delivered to user's email address.
  - **Microsoft Authenticator application** - for use with mobile devices running Android or iOS platforms. The application generates 6-digits access code every 30 seconds.
- **Security Key** - Passwordless authentication method allowing users to authenticate using devices such as YubiKey, USB token, smart phone fingerprint or Windows Hello. User authentication is verified via PIN code, biometrics or other factors that securely verify user's identity.

## Multi-factor Authentication Logon Experience

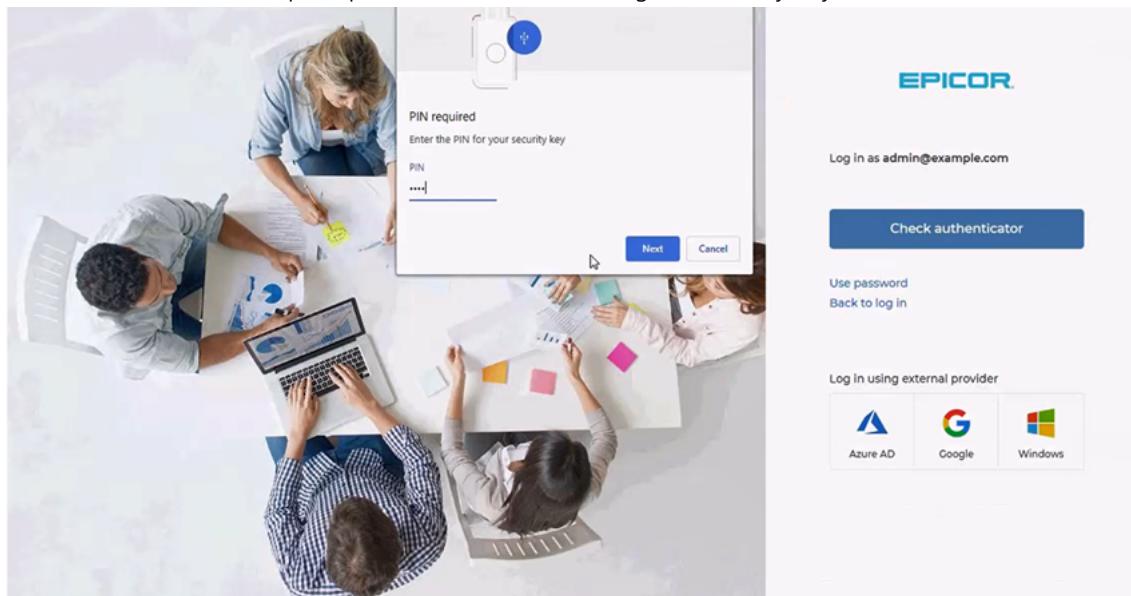
This topic highlights various Multi-factor authentication (MFA) implementation scenarios.

### Passwordless login enabled

- Multi-factor authentication is enabled for a tenant.
- A user creates new Security Key in Account Settings page.
- On the next logon, the option to Log in without password displays for the user.



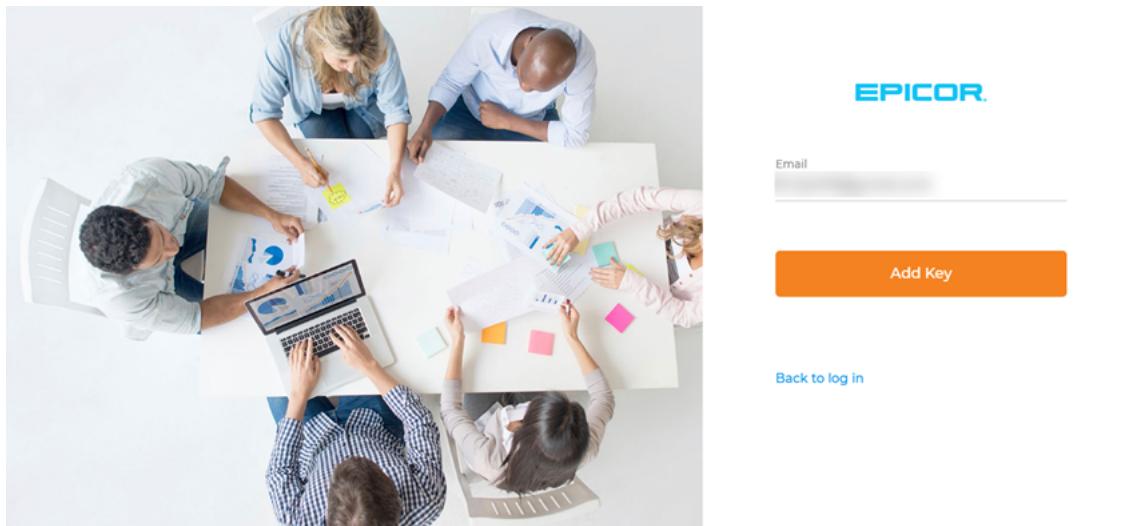
- When selected, a user is prompted to authenticate using the security key.



- A user may toggle between using a password or Passwordless authentication as needed.

### Passwordless Login Required

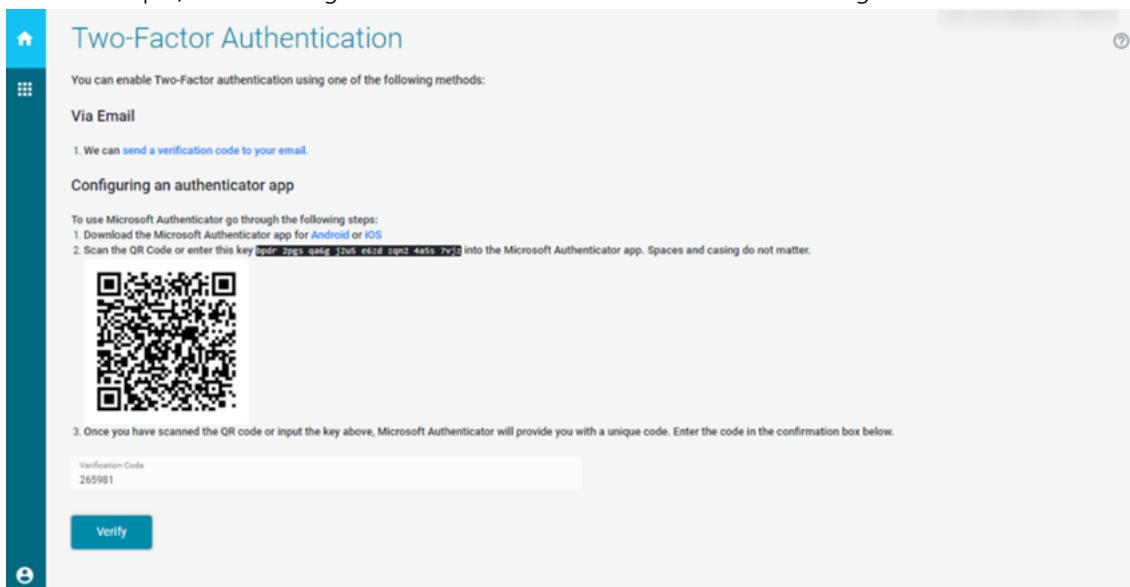
- On the initial logon, a new user is asked to create a new Security Key instead of a password. Once registered, a user is prompted to authenticate using the key.



- The new key is named Default and displays in the list of user's Security Keys.

### Multi-factor authentication enabled

- A user navigates to My Account > Two-Factor Authentication page and Enables two-factor authentication. Based on which MFA authentication methods were made available for a tenant, a user Configures authenticator (through Verification Code email delivery or by downloading Microsoft Authenticator application to a mobile device) and/or creates a new Security Key for use with Passwordless Authentication.
- In this example, a user configured One-time access code MFA method using the **Authenticator**.



- On the next logon, a user is first asked to provide an email and password. The following screen asks the user to authenticate using the Authenticator code. The code may be retrieved using the Microsoft Authenticator application from user's mobile device, or it may be delivered to user's email address. If necessary, a user may log in using one of the generated recovery codes.



### Multi-factor authentication required

- On the initial logon, a user is first asked to create a new password.



- Once the new password is set, depending on the available MFA tenant methods, a user is asked to either create a new Security Key or to configure the Authenticator.



- In this example, a user decided to configure the Authenticator. The Verification Code may be delivered to user's email address or retrieved using the Microsoft Authenticator application a user needs to download and install on a mobile device.



- Upon successful Authenticator configuration, a user is asked to log in using the new password followed by an Authenticator code.



## Documentation Resources

For more information on Epicor Identity Provider, review the below documentation resources.

- **Epicor Identity Provider User Guide** - found in ERP Application Help under **System Management > Working with System Management**.
- **Epicor IdP Help** - accessible from within the IdP application.

A screenshot of a web browser displaying the 'Two-Factor Authentication' article from the Epicor Identity Provider Help system. The browser's address bar shows the URL 'epicorapplications.zendesk.com/hc/en-us/articles/360044771412-Two-Factor-Authentication'. The page itself has a blue header bar with the title 'Two-Factor Authentication'. The main content area contains navigation links like 'Identity Provider Administration', 'My Account', 'My Applications', and 'Release Notes'. The main text discusses the safety benefits of 2FA and lists supported authentication methods. A red arrow points from the left margin of the page towards the browser's address bar.

- **Epicor Identity Provider ISV Documentation:**
  - **External** audience: <https://developer.epicor.com/erp-isv-home/developer-center/epicor-identity-provider/getting-started/>
  - **Internal** audience: <https://developer.epicor.com/epicor-internal-developers/epicor-identity-provider/>



## Authorization - Interface Security

You control access to the Epicor ERP user interface through the internal security functionality. By identifying which users need and do not need access to various programs, you ensure the integrity of the data entered in the application.

You can first restrict access to various parts of the Menu through run time arguments. By adding a Menu ID run time argument to a desktop icon, the Epicor ERP application will only display the programs available under this specific Menu ID.

If you have more comprehensive security requirements, you define internal security for your application through two key programs. First, use Security Group Maintenance to create groups that identify user related areas within your organization. Then assign all users to these security groups through User Account Maintenance. With security groups and their selected users defined, you can then assign security privileges throughout the application. For example, you may want to prevent access to Payroll programs for most users. You can use the security privilege tools to only give members of the Payroll security group access to these programs.

You define security access through three maintenance programs. Menu Maintenance can prevent programs from being displayed for specific security groups and users. To block access to a program or program function (like updating records) from wherever it can be launched, use Service Security Maintenance. You can also block or limit access to a specific field by using Field Security Maintenance.

To review security settings and user activity, you run reports. The Menu Security report displays the current access rights specific users and security groups have on the Menu. Other reports are available that display user activity, so run these reports to verify the security settings you defined work as expected.

## Security Privileges

This section of the guide details how you assign security privileges for users. These privileges define the level of access each user has in each company.

### Company Security

If your organization has multiple companies, you will need to set up security separately within each company. The users within each company will then access the Epicor ERP application using the security plan you have defined.

Note each database will have at least one company in it. During installation, the Epicor ERP application automatically creates a blank company (TEST) and a single user (EPICOR) with Security Manager privileges in every database. You can then successfully log into the Epicor ERP application for the first time.

### Security Group Maintenance

Use Security Group Maintenance to establish security groups that define various functions either throughout your organization or for a specific company. You then use these security groups to assign or limit access to various areas within the Epicor ERP application.

You can assign a user to a security group in User Account Maintenance, and then you can select security groups on various security sheets in other programs. While optional, security groups are useful because they can categorize employees by role or department.

Epicor recommends you create security groups and assign all users to specific groups. You then simplify your security setup, as you do not need to assign security to individual users. This approach also ensures you implement security through an organized and clearly defined method.

Before you begin assigning security, consider the various areas of security your company needs. You should then design a security plan and enter security groups that reflect this plan. While you set up this plan, consider that roles tend to be more generic, while job titles tend to be more specific. Several job titles can fulfill the responsibilities of a single role.

### Create a Security Group

1. Navigate to **Security Group Maintenance**.

**Menu Path:** System Setup > Security Maintenance > Security Group Maintenance



**Important** This program is not available in Epicor Web Access.

2. Click **New**.

3. In the **Group Code** field, enter an identifier you will use for this new security group.

4. In the **Description** field, enter a short explanation for the security group. This text displays within the security programs, so be sure to enter a value that helps you identify the purpose of this security group later.



**Tip** If you place an underscore (\_) or a period (.) in front of the Description, the security group sorts to the top of the list in the security programs. This makes the new security group much easier to find.

5. Click **Save**.

## 6. Exit Security Group Maintenance.

This new security group is now available. You first assign users to this security group. You can then select this security group in the security programs.

### User Security

Launch User Account Security Maintenance to assign users to both security privileges and security groups.

The security privileges give a specific user access to various Epicor ERP application features. For example, you can give a user access to the customization tools, but not allow this user to make language string changes. You can also give a user Security Manager rights; this user can then modify security settings for other users.

Through the security group functionality, you can assign a single user to multiple security groups. When you allow or disallow a security group on security sheets in other programs, the users assigned to this security group will either have access or have no access to functionality assigned to the security group.

### Security Manager Levels

The Security Manager and Global Security Manager rights are special permissions granted to certain users. If your user account has either of these rights, you can define security levels to restrict modules, programs, methods, or fields to specific users and/or security groups.

#### **Security Manager Rights**

The Epicor ERP application restricts access to the System Setup module; the programs used to create a security strategy are available within this module. Epicor creates a single user (manager) with security manager privileges in every database. This default record is created during installation, and you use this account to create user account records - including other accounts that have the Security Manager status.

As a good business practice, you should not give yourself Security Manager access on your normal user account. This ensures the menu choices you make on your normal login are appropriate for your typical daily routine. It also ensures that other employees do not grant security access to themselves when you are away from your computer. Instead, create a separate Security Manager account that you only use for security tasks.

#### **Global Security Manager Rights**

Some user accounts can have Global Security Manager rights. This option is used to address security needs in multi-tenant environments such as Epicor Express and SaaS Standard. For most installations, you will not be able to grant global security manager rights. Administrators assign this status to a group of users within the Epicor Administration Console, or individually through User Account Security Maintenance. If you are in an environment where you cannot launch the Epicor Administration Console, this security level is not available for your use.

Global security managers have the highest level security in the Epicor ERP application (and other ICE applications). Global security managers can access companies across tenants in an Epicor hosted environment. They can be added to specific companies, regardless of the tenant, to administrate them. These users also have Security Manager rights. Because of this, they can prevent all other users, including users with Security Manager rights, from accessing a specific menu or program.

Internal Epicor administrators who need more information should refer to the Epicor SaaS Installation Guide.

### Assign Security Privileges

You assign security privileges to a user within User Account Security Maintenance. You assign these rights on the Options sheet.

#### **1. Navigate to [User Account Security Maintenance](#).**

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

2. In the **User ID** field, enter the identifier for the user account for which you need to assign security.
3. You can limit what this user sees on the Main Menu by entering a value in the **Client Start Menu ID** field.

When this user launches the Epicor ERP application, only the contents under the specific sub-menu identifier or the specific program appear on the Main Menu.



**Tip** You can find the specific menu identifier you need within Menu Maintenance.

4. Click on the **Options** sheet.
5. Notice the **Security Manager** check box.

Users with this security access can define and change the profiles of themselves and other users. They can also access all security programs; only select this option for user accounts that will handle security tasks.



**Note** As described previously, some users may also have Global Security Manager rights. This level of security is reserved for Epicor hosted environments such as Epicor Express and SaaS Standard, so typically you do not implement security through this access level.

If you are in a hosted environment, you can individually add or remove Global Security Manager rights within User Account Security Maintenance. Click the List sheet and select/clear the Global Company Security Manager check box. If you de-activate Global Security Manager rights, the current user can still have Security Manager rights. However you cannot clear this check box if the user has access to multiple tenants; you must first remove this user from the other tenants before de-activating Global Security Manager rights.

6. Activate the **Allow Session Impersonation** check box so the current user account can be selected on system agent and task agent services.

To do this, you enter this user account in **System Agent Maintenance** on the Detail sheet; place this User Name and Password in the System AppServer section. You later enter this user account on the task agent in the **Task Agent Service Configuration** program; you access this program on the application server in the Epicor Administration Console. The user can then log into these services.

This user can also run all the report and process tasks assigned to schedules on this system agent. Normally only the users who added the report and process tasks to a system agent schedule can run them. However a user assigned these rights can impersonate all the users who have assigned tasks to the system agent, and can run these tasks as needed.

7. The **Tools Options** group box contains permissions for customization, SQL Server Reporting Services (SSRS), Business Process Management (BPM), Business Activity Query (BAQ), searches, and other system tools. Select the tools that will be available through the current user account.
8. The **Access Options** define what additional interfaces are available through this user account. You can activate Enterprise Search, Epicor Web Access (EWA), and Mobile Access through these options. You can also give this user the rights to change the account password.
9. Use the **System Options** to indicate how this user account interacts with the system. You can give this user rights to launch multiple sessions of the Epicor ERP application, add Main Menu tabs and Favorites, save reports and modified interface layouts when the user exits, and create help annotations.
10. If you need, use the **Enterprise Search** fields to override the Epicor Enterprise Search installation. This user account can then access Enterprise Search through a different URL.

11. The **UI Options** give the user access to features that change the look and feel of the interface. Through these options, the user can create custom Home Page Layouts for the Modern Shell interface and create/edit interface themes.

12. Click **Save**.

This user account now has access to the privileges you selected.



**Tip** If you need more information on each permission, review the User Account Security Maintenance topics in the application help or the Personnel chapter in the Implementation User Guide.

## Assign Security Groups

You can now assign this user account to a specific security group or groups. When you grant or prevent access through this security group, this user account then uses this access setting.

1. Navigate to the **Group** sheet.

The **Available** list displays the security groups available in the application.

2. Highlight the security group you want to assign to this user.

3. Click the **Right Arrow** button.

The security group now moves to the **Authorized** list.

4. Click **Save**.

The current user account is assigned to the selected group or groups.

## Security Logic Hierarchy

The Epicor ERP application contains a security logic hierarchy that determines access to each menu, program, service, method, or field. Before you implement security on these items, be sure you understand this hierarchy to prevent unexpected results.

The following list defines the security logic hierarchy in descending order. The security logic is based on user account permissions. If a user account matches the security logic at one level in this hierarchy, the Epicor ERP application applies that level of security to the user account, overriding the lower levels in this hierarchy.

1. If the user account has **Global Security Manager** rights, this user can access companies across tenants in an Epicor hosted environment. They can be added to specific companies, regardless of the tenant, to administrate them. This level of security is reserved for Epicor hosted environments such as Epicor Express and SaaS Standard, so typically you will not implement security through this access level. Global security managers can prevent security managers from accessing sensitive programs and menus in hosted environments.
2. If the user account has **Security Manager** rights, few (if any) security restrictions are applied against this account. This user typically has full internal access to the entire Epicor ERP application. As described previously, security managers may not have access to some programs and menus in Epicor hosted environments. However you typically implement security through a user account with Security Manager rights.
3. When a specific user account is denied access to a menu, program, service, method, or field, this user account cannot use this item.
4. When a specific user account is granted access to a menu, program, service, method, or field, this user account is able to use this item.

5. If a user is assigned to any security group that denies access to a menu, program, service, method, or field, the user cannot use this item.
6. If a user is assigned to any security group that allows access to a menu, program, service, method, or field, the user is able to use this item.
7. When no other security restrictions are in place, the default security permission on the column determines whether access is granted or denied on this specific column.



**Note** Notice that user account permissions override security group permissions. Through this feature you can assign unique security access for specific users while still including them in security groups.

Once you determine which users and security groups should and should not have access to specific areas of the Epicor ERP application, you are ready to define access within Menu Maintenance, Service Security Maintenance, and Field Security Maintenance.

## Assign Security

You can assign security to programs, services, methods, and fields.

You assign security through the following features:

- **Run Time Arguments** - Limit access to a specific menu node on a client installation.
- **Menu Maintenance** - Use security groups and user accounts to prevent or allow access to specific programs.
- **Service Security Maintenance** - Use security groups and user accounts to prevent or allow access to specific services (business objects such as customers, parts, sales orders, and so on) and/or methods within these services (like Get New, Update, Delete, and so on).
- **Field Security Maintenance** - Use security groups and user accounts to prevent or allow access to specific fields in programs.

### Run Time Argument Menu Control

You can assign security on specific desktop icons by using run time arguments. Use this functionality to limit the programs that display when users launch the Epicor ERP application.

This security functionality is an effective way to quickly set up a level of security on workstations. You do not need to use security groups or user accounts with this functionality. Each workstation can have a number of desktop icons available for launching the Epicor ERP application. Each desktop icon can in turn be set up to launch the Epicor ERP application in a specific mode defined by a run time argument.

You can use the /MENUID run time argument to cause the Main Menu to only display a specific sub-menu or program. The user who launches the Epicor ERP application through this icon is limited to the programs accessible within either the menu or the specific program.

You can also use the /TE and /CRM run time arguments to set up unique concurrent user licenses. The /TE argument limits the Main Menu to display only the Time and Expense functionality, while the /CRM argument limits the Main Menu to display the Customer Relationship Management functionality. These unique licenses consume a different concurrent user pool. Activate these licenses either when you want to limit a workstation to display only these specific functions or when you want to set up additional licenses separate from the general user pool.



**Tip** The security features available through run time arguments are described in this section. For information about other options, review the Run Time Arguments section later in this guide.

## Define Run Time Arguments

To leverage this feature, you display the Properties window for the Epicor shortcut icon and then modify the Target field to include a menu ID.

1. On the desktop for the workstation, right-click on the application's icon; from the context menu, select **Properties**.

The application's Properties window appears, displaying the **Shortcut** tab.

2. In the **Target** field, add a dash (" - ") and enter the identifier for the menu or program that you want to display.



**Example** For example, to restrict the workstation to display only the CRM module, enter: -menuid =CRMN0000

3. Click **Apply**.

4. Click **OK**.

5. Launch the Epicor ERP application through this icon.

The **Log in** window displays.

6. Select the **Classic Style** check box.



**Important** The MENUID run time argument only works with the Classic Style interface. It does not restrict menu access in the Modern Shell interface.

7. Enter a user account.

The Main Menu only displays the programs available under the Menu ID you entered for the shortcut.

The -menuid method may not limit access to all the programs you intend. Several programs can still be launched by right-clicking various fields. For example, users could still launch Part Maintenance from the Part field's context menu. If the modules that contain these programs are licensed in your Epicor ERP application, users will be able to access them through context menus. You will need to use other security methods to restrict access to the programs available on context menus.

## Menu Security

Use Menu Maintenance to define security options for users in the current company.

Menu security is the highest level where you can set security privileges. You can use the security in this management program to hide a program or a folder on the Main Menu from security groups or specific users. Changes you make in this program display on all the workstations that run the application.

Module groups and modules are organized by folders. Module function categories, such as Setup, General Operations, and Reports, are also organized by folders. Most menu folders, except those in the System Management module group, are initially available to all users, so you have a lot of flexibility determining which users have access to different parts of the Menu.



**Important** You can only use this program if your user account has customization rights.

## Create a Security Code

You first use Menu Maintenance to create a security code. You then indicate which users have access to this code.

1. Navigate to Menu Maintenance.

**Menu Path:** System Setup > System Maintenance > Menu Maintenance



**Important** This program is not available in Epicor Web Access.

2. Click the **Down Arrow** next to the **New** button and select **New Security**.
3. In the **Security ID** field, enter an identifier that helps you locate this security group later.
4. In the **Description** field, enter a concise explanation for this security code.  
This value briefly describes the purpose of the security code.
5. The **Owning Company** field displays the company in which the current security ID was created; you cannot change this value.
6. Typically you select the **All Companies** check box. This indicates users within companies in the same organization as the Owning Company can view and use this security ID. However only users within the Owning Company can make changes to it.  
 **Note** If the System check box is selected, the Owning Company field is blank. This indicates the current security setting is available to all companies within your organization.
7. If you select the **Global Security Manager Only** check box, only the Global Security Manager access a menu item assigned to this security ID.  
This check box prevents all other users, including users with Security Manager rights, from accessing the selected menu or program. This option is the highest level security available in the Epicor ERP application, and is used to address security needs in Epicor hosted environments. For most installations, you can ignore the Global Security Manager Only check box. You assign Global Security Manager rights to users within the Epicor Administration Console.
8. If you select the **Security Manager Only** option, this security ID blocks all access to the programs and menus assigned to it.  
This option is useful when you are first setting up security, as it blocks all access until you create a security plan. As described previously, you assign security rights to user accounts within User Account Security Maintenance.
9. Select the **Exclude Epicor Web Access** check box to indicate modules and programs assigned to this security ID will not display as a web form in an Epicor Web Access (EWA) environment.  
When you select this check box, EWA users cannot access any menu items assigned to this security ID. These programs will also not display for both Global Security Managers and Security Managers; these users will need to launch these programs through their smart client interface.
10. Navigate to the **Allow Access** sheet.



**Important** You can use either the Allow Access and Disallow sheets to assign security; the Allow Access method overrides the Disallow Access method. If a user is assigned to both sheets, the user has access to the programs assigned to this security code.

11. Clear the **Allow Access to All Groups/Users** check box.

12. Click **Save**.

The **Groups/Users** and **Selected Groups/Users** lists become active. Now until you add users and/or groups to the Selected Groups/Users list, nobody has access through this security level. Be sure you are ready to assign security before you clear this check box.

13. Highlight the specific group or user for which you want to give security access.

14. Click the **Right Arrow** button.

The user or group displays on the Selected Groups/Users list.



**Important** Any groups or users that remain in the Groups/Users list do not have access to the programs assigned to this security level.

15. Click **Save**.

Groups or users in the Selected Groups/Users list have access to the programs assigned to this security level.

## Assign Menu Security

When you assign a security code to a selected program, only those users given access through this security code can launch the program.

1. Navigate to the **Detail** sheet.

2. Now from the tree view, select a program.

3. Click the **Security ID...** button to find and select your security code.

The **Security ID...** field now displays the new security level you have selected.

4. You can also review which programs are assigned to this security code. To do this, return to the Security sheet and find/select a security code.

The **Menu Options** field displays the programs that currently use this security code.

5. Click **Save**.

This program is assigned to this security level.

## Security Group Conflicts

The application handles conflicts between security groups through an access hierarchy.

1. If a user is assigned to security group \_Production Staff, which allows access to the Engineering Workbench, and security group Purchasing, which does not, the user will still be able to launch the Engineering Workbench. The security group with more access overrides the security group with less access.
2. Likewise, if a user is assigned rights to a program, but is assigned to a security group which is not, the user is still able to launch the program. User rights have precedence over group rights.

3. The **Allow Access** mode also has precedence over the **Disallow Access** mode. You select these modes in the Menu Maintenance, Service Security Maintenance, and Field Security Maintenance programs.

## Service and Method Security

You launch Service Security Maintenance to establish security at the service level and at the method level within a service.

Use the **Service** sheet to set the security privileges for services (business objects) like Customers, ABC Codes, Tax Regions, and other services. Use the **Method** sheet to establish security at the method level within a service. A method is an action that can be taken in a service such as Update, Get New, Approve, and so on.

 **Example** The Terms service (Business Object) displays on the menu in several places and it can also be accessed within Company Configuration and other programs. If you want to block access to specific users and security groups from all locations on the Menu screen, you would limit it at the service level (BO.Terms) on this Service sheet. If you want to block the ability for some users to Update existing Terms codes, you would limit access at the Method level (BO.Terms.Update) on the Method sheet.

When a service is secure, all methods within this business object are also secure. This can lead to unexpected results, as the methods will not run through Service Connect, embedded services, and from other menu options. Epicor recommends you assign security in a test environment first before you deploy security within your live environment.

### Assign Service (Business Object) Security

You define security for a service by first selecting it and then indicating which groups/users can and cannot access it.

Like Menu Maintenance, you can use either or both sheets to assign security; remember that the Allow Access method overrides the Disallow Access method. If a user is assigned to both sheets, the user has access to this service.

1. Navigate to **Service Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > Service Security Maintenance

 **Important** This program is not available in Epicor Web Access.

2. Click **New**.

3. Click the **Service ID...** button to find and select the service you need.

4. The **Owning Company** field displays the company in which the current service security setting was created; you cannot change this value.

If the **System** check box is selected, the Owning Company field is blank. This indicates the current security setting is available to all companies within the current organization.

5. Click on the **Allow Access** sheet.

6. Clear the **Allow Access to All Groups/Users** check box.  
This indicates no users have access to this business object.

7. Navigate to the **Disallow Access** sheet.

8. Verify the **Disallow Access to All Groups/Users** check box is clear (not selected).

Now until you add users and/or groups to the **Selected Groups/Users** list, everyone has access to this business object. Be sure you are ready to assign security before you clear this check box.

9. From the **Groups/Users** list, highlight the security group you want to use.
10. Click the **Right Arrow** button.  
The security group displays on the Selected Group/Users list. Now only users assigned to this security group cannot access this service.
11. Click **Save**.

## Assign Method Security

You can also use Service Security Maintenance to define security for methods within a selected service (business object).

A method is an action which can be run within a service like Update, Get New, Approve, and so on. For example, you can use this functionality to permit a user to add a release to an existing purchase order but prevent this same user from creating a new purchase order.

 **Tip** Not all services (business objects) have multiple methods. This sheet is only for more complex services that perform a variety of actions.

1. Click **New**.
2. Click the **Service ID...** button to find and select the service you need.
3. Click the **Down Arrow** next to the **New** button; select **New Method**.  
The **Method** sheet becomes active.
4. From the **Method Name** drop-down list, select a method.
5. The **Owning Company** field displays the company in which the current method security setting was created; you cannot change this value.
6. If you wish, select the **All Companies** check box.  
Now users within companies in the same organization as the Owning Company can view and use this method security setting. However only users within the Owning Company can make changes to it.
7. Navigate to the **Allow Access** sheet.
8. Clear the **Allow Access to All Groups/Users** check box.  
Until you add users and/or groups to the **Selected Groups/Users** list, nobody has access to this method. Be sure you are ready to assign security before you clear this check box.
9. Click the **Double Right Arrow** button.  
All the users and security groups move to the **Selected Groups/Users** list.
10. From this list, highlight the security group you want and click the **Left Arrow** button.  
The security group displays on the **Groups/Users** list. This security group does not have access to the current method.
11. Click **Save**.

## Field Security

Use Field Security Maintenance to establish security privileges at the field level in specific database tables, extended user defined tables, and fields throughout the application.

Field Security Maintenance contains functionality you leverage to define security privileges on fields for all users, selected users, and groups. You use this program to first select a table and then allow, limit, or prevent access to specific fields within the selected table. Each field can have a unique security level assigned to it; this level can be globally defined for the whole organization, specifically defined for the current company, or specifically defined for a selected user or group.

You can reset the security privileges for a selected field or the whole table to the default values initially granted all users. You can also view the security privileges for the fields in the table for the selected user.

Be sure you set up user accounts and security groups before using this program.

 **Important** Table and field security can only be applied to actual database tables and columns. Use customization to secure temporary table information. You can also use Business Process Management method directives to secure temporary tables. The application's Field Help displays several pieces of information including the External check box. If the External check box is selected and no data displays for the database field, this is a Calculated Column or belongs to a temp table.

You can use Extended Properties Maintenance to verify the table type. If the dataset table is temporary, Temp Table displays in the Table Type field. Use the Fields > Detail sheet to determine if the field is External. Typically, temp tables have a Like value that points to the actual table or column used to retrieve and store the data.



**Example** The SrcGLTran table is a temp table and not an actual database table.

## Assign Global Field Security

You can assign security to a specific field that then applies to the entire organization or a specific company.

1. Navigate to **Field Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > Field Security Maintenance



**Important** This program is not available in Epicor Web Access.

2. Click the **Schema** drop-down list and select the Erp schema option.

3. In the **Table** field, enter a table name and press **<Tab>**.

The **Description** field displays the purpose of the selected table.

4. In the tree view, select a field.

The **Field Name** displays the name of the selected field.



**Tip** If the **Primary Key** check box is selected, it indicates the current field is required by the database. You cannot change the security option for a Primary Key field; usually these fields are for identifiers like the Customer ID, Part ID, and so on.

5. Click the **Default Access** drop-down list; select one of these options:

- **Full** - Users can both view and enter data within this field. This security option is the default.

- **Read** - This option assigns display-only (read-only) rights to the current field. Users can only view data within this field; users cannot enter data within this field.
- **None** - This security option causes the field to be blank. No data displays in this field, and users cannot enter data in it. Be aware that the None setting also causes the field's data to not be included when the dataset is sent to and from its program. This can have unintended consequences for processes, like BPM directives, which may require this data.

**6.** The **Owning Company** field displays the company in which the current field security setting was created; you cannot change this value.

**7.** Select the **All Companies** check box.

Now users within companies in the same organization as the Owning Company can view and use this field security setting. However only users within the Owning Company can make changes to it.

**8.** Click **Save**.

Now users can only review the text in the selected field.

## Security Group Field Security

You can also assign security to a field that only applies to a specific user or security group.

**1.** Navigate to the **Users/Groups** sheet.

**2.** In the grid, select a security group.

**3.** In the **Tree View**, select a field.

**4.** Click in the **Access** column to display the drop-down list and select one of these options:

- **Full** -- Users in this security group can enter data in this field.
- **Read** -- Users in the current security group can review the data in this field, but they cannot enter data in this field.
- **None** -- This security option causes the field to display as blank for all users in this security group. No data displays in this field, and users cannot enter data in it. Be aware that the None setting also causes the field's data to not be included when the dataset is sent to and from its program. This can have unintended consequences for processes, like BPM directives, which may require this data.
- **Default** -- Select this option when you want the user or security group to use the global security level assigned for this field on the Detail sheet.

**5.** Use the **Tree View** to continue to select other fields from the list.

**6.** When you finish setting up security for these fields, click **Save**.

Now when a user in the selected security group logs in, the fields use the access settings you assigned to them.

## Security Management

You can use the Menu Security report to review the security settings defined for your organization and the System Activity Log to monitor user database activity. Other security reports are available that help you manage user and security group activity.

Each report displays a specific view of user activity. Use these reports to evaluate your security settings and practices.

## Change Log Report

The Change Log report displays activity that occurred in the database during a specific period of time. Leverage this report to see what changes users are making to the database.

When you need to find out where and when data was changed in specific tables, run this report. For example, you may need to run this report to help conduct an audit or identify problems with database security. You can limit this report to only display database activity entered in a selected table or a series of tables.

Use the **Selection** sheet to select the report parameters. Use the **Filter** sheet(s) to select the specific records to include on the report. For more information, refer to the Filters Overview topic in the Application Help.



**Important** For more information on how to review the status of a report you print, preview, or generate, refer to the System Monitor Overview topic in the Application Help.

### Menu Path

Navigate to this program from the Main Menu:

- Executive Analysis > Business Activity Management > Reports > Change Log Report
- System Setup > Security Maintenance > Change Log Report

## Logon Failure Audit Report

Use the Failed Logon Audit Log Report to review invalid logon attempts during a date range you define.

This report audits failed user account logon activity. It displays the invalid user account, password, and the date/time the attempt occurred. This audit report does not have additional filter options.

Use the **Selection** sheet to select the report parameters. Use the **Filter** sheet(s) to select the specific records to include on the report. For more information, refer to the Filters Overview topic in the Application Help.



**Important** For more information on how to review the status of a report you print, preview, or generate, refer to the System Monitor Overview topic in the Application Help.

### Menu Path: System Setup > Security Maintenance > Logon Failure Audit Report

## Menu Security Report

Generate the Menu Security report to review the current access users and security groups have on the Main Menu.

Run this report to evaluate the security currently defined for your programs. You can review the security for users, security groups, or both. You can also filter this report to only display access for a specific program, user, or security group. This key report can give you a complete overview of the security plan currently in place.

Available controls:

- Use this **Selection** sheet to choose the parameters for the report.
- Use the **Filter** sheet(s) to select the User and Security Group to include on the report.



**Important** For more information on how to review the status of the reports/forms you print, preview, or generate, review the System Monitor topic in the Interface Navigation section of online help.

### Menu Path: System Setup > Security Maintenance > Menu Security Report

## System Activity Log

Use the System Activity Log dashboard to review all database modifications that occurred within the application.

This valuable tool can help you determine where and when specific database changes were carried out and who initiated these changes. You can locate the database activity you wish to review by filtering the data activity that displays through the available search fields.

To use this log, you first need to activate it within **Company Maintenance**. As users make changes to the database, this log records these entries. You then launch the System Activity Log and review this database activity by filtering on a specific user, date range, both user and date range, or other options. Later you remove selected entries from this dashboard by running the **System Activity Log Purge** program.

**Menu Path:** System Setup > Security Maintenance > System Activity Log

## Users/Groups Report

Run the Users/Groups report to review the current list of users assigned to security groups in the current company.

Although you can run this report to display all security groups and users, you can also limit this report to display the users assigned to a specific security group or the security groups assigned to a specific user.

If you use this report in a SaaS (Software as a Service) environment, you can only review users and security groups available in your tenancy. However if you are a Global Security Manager, you can run this report to display users and security groups for all companies you manage, across all tenancies.

 **Tip** The options/values for tenant and multi-tenant features are only for Epicor hosted environments. Typically you can ignore these options. Internal Epicor administrators who need more information should refer to the Epicor SaaS Installation Guide.

Use the **Selection** sheet to select the report parameters. Use the **Filter** sheet(s) to select the specific records to include on the report. For more information, refer to the Filters Overview topic in the Application Help.

 **Important** For more information on how to review the status of a report you print, preview, or generate, refer to the System Monitor Overview topic in the Application Help.

**Menu Path:** System Setup > Security Maintenance > Users / Groups Report

## User Session Log Report

Run the User Session Log report to review how often all users or a specific user accessed the Epicor ERP application.

You enter a date range and can optionally select either all users or a specific user. The report displays the Log on and Log off date/time record for each time the user accessed the Epicor application. Run this report to help conduct an audit or identify problems with database security.

Use the **Selection** sheet to select the report parameters. Use the **Filter** sheet(s) to select the specific records to include on the report. For more information, refer to the Filters Overview topic in the Application Help.

 **Important** In **Epicor Cloud ERP - Multi Tenant** or **Epicor Cloud ERP - Dedicated Tenancy**, this program or feature may not be available or may operate under certain restrictions.

 **Important** For more information on how to review the status of a report you print, preview, or generate, refer to the System Monitor Overview topic in the Application Help.

**Menu Path:** System Setup > Security Maintenance > User Session Log Report

 **Important** This program may not be available, or operate under certain restrictions in Epicor Cloud ERP.

## Configuration Settings File

When you launch a client installation, it activates the configuration settings file. This file defines the main settings for your server installation and each client installation.

The application cannot launch unless it locates a configuration settings file. If the .exe file can see the **default.sysconfig** file (or an alternate file), the application launches.

The configuration settings file is an XML file that contains various settings. These settings define the parameters used by the client installation. If you need, you can modify the file to address the needs of both your network and a specific user. This section explains how you modify the default.sysconfig file. You can also review a complete list of the available settings and their options.

### File Customization

You can customize this configuration settings file to both match your network and the parameters needed for a specific client installation.

You can modify this file to personalize the overall settings for the application on each client machine. A key setting you can change is the **CultureCode** value; it causes the application launch in a different language. You can also define the **LoginDefault** value to indicate the default **user name** value that appears on the **Log On** window. You can even set up this file to skip the Log On window completely and automatically launch the application.

The configuration settings file adjusts how each client interacts with the server as well.



**Example** If you want your .htm pages hosted on a separate server than the deployment server, you would enter the specific server url in the Url attribute. When a user double-clicks the desktop icon, the default.sysconfig file (or alternate file) activates. The application launches on the client machine using the new url setting.

By changing just a few parameters within this file, you can improve user experience with the application and modify how each client interacts with the overall network.



**Important** Before you modify this file, you need to understand your network. If you are not sure about customizing this file, work with your consultant before you make any changes.

### ConfigEditor Tool

The **ConfigEditor.exe** tool provides a graphical interface for adjusting the configuration settings.

Use this tool if you are more comfortable working with a window instead of a text editor like **Notepad**. Each setting within the file displays as a separate field. When you save the changes entered in each field, you update the configuration settings file.

## Configuration Settings File Functionality

The following topics explain how to use the Configuration Settings File functionality.

### Default.sysconfig File

The Configuration Settings File is located in the **Config** folder within the client application's files.

Its filename is **default.sysconfig**; you can open this file within any text editor. It is located in the following path:

- ..\Config\default.sysconfig

After you open the file, you will notice that it uses **.xml** tags for each setting. The settings are first divided into primary tags like **<userSettings>** and **<helpSettings>**. Within each primary tag, there are specific setting tags that you can change. For example:

- <CultureCode value="enu" />

The **CultureCode** value defines the xml tag. For this setting, the tag defines the language used on the client machine. The variable, **enu**, is displayed within the quotation marks and indicates the specific language that will be used. In this example, the log on file will display the application using the English language.

You use this syntax for each setting. Modify the variable within the quotation marks to adjust a default log on value for the client or server application.



**Important** Be sure you understand what you are modifying before you save this file. If you change a variable incorrectly, the application may not work as expected. If this happens, restore this file's default settings.

### Use the ConfigEditor Tool

Follow these steps to use the ConfigEditor Tool.

1. Open **Windows Explorer** and navigate to your client folder (for example, C:\Epicor\EpicorERP\client).
2. Double-click **ConfigEditor.exe**.
3. In the dialog that displays, select a .sysconfig file to adjust (for example, default.sysconfig).
4. Select the tab that contains the setting you need to change.
5. Enter information in the field.
6. To save settings at any time, click **Save**.
7. When you finish, click **Close**.

The configuration settings file is updated with your changes.

## Configuration Settings List

This series of tables list all the settings available within the default.sysconfig file. Each primary tag has its own table. Within each table, the specific setting tag, its definition, and its expected value are documented.

### Application Settings

The Application settings contain general connection settings and configuration settings.

You change these settings to apply custom (OEM) style themes to the application. You can also define custom images and text through these settings.

Typically system administrators define these settings and then distribute the updated configuration files to all workstations within the network for which they apply.

If you use Cloud or a similar Epicor hosted environment, you can copy and paste any of the **<appSettings>** settings into the **<userSettings>** node within the same .sysconfig file. You can then enter the value you need within the copied setting. When users launch the hosted application, it first checks the **<userSettings>** node for Application setting values. By default, the hosted application first loads any settings it finds in the **<userSettings>** node instead of the **<appSettings>** node. This prevents the MES menu and other parts of the hosted application from reverting back to the default .sysconfig settings each time a new version of the software is released.

XML Tag	Purpose and Expected Value
AppServerURL	<p>Displays the <b>AppServer Uniform Resource Locator</b> (URL) that connects the task agent to the application server (AppServer). If you need to locate this URL, open the *.sysconfig configuration file for your application and locate the AppServerURL node. Typically this file is found in the <b>client &gt; config</b> folder of your Epicor client installation.</p> <p>For example, your AppServer URL may look similar to the following: net.tcp://&lt;app server name&gt;/ERP10/</p>
AlternateCacheFolder	<p>The location of the local disk cache folder. This folder is used to hold cached .xml files. If none is specified, the default is C:\ProgramData\Epicor</p> <p>This folder accommodates some environment variables which can be substituted during startup.</p> <ul style="list-style-type: none"> <li>• <b>%UserName%</b>— The Windows ID of the user. For example, jsmith</li> <li>• <b>%UserDomain%</b>— The Windows user domain. For example, USEAST</li> <li>• <b>%AppData%</b>— The application data folder. For example, C:\Users\jsmith\AppData</li> <li>• <b>%Homepath%</b>— The home path folder. This location is specified in Local Users and Groups. For example, C:\Users\jsmith</li> <li>• <b>%AllUsersProfile%</b>— The location of the All Users profile. For example, C:\Users\Public</li> </ul>

XML Tag	Purpose and Expected Value
CultureCode	<p>The ISO language/culture code that defines the specific language and format which displays on the <b>Logon</b> window. For example, "sch" (Simplified Chinese).</p> <p>This value only affects the Logon window. After the user enters a user name and password and clicks past this window, the language and culture code settings defined on the user account appear within the Epicor application.</p>
CustomResourceFile	<p>A path name to a resource file that contains custom images. You can add images to this file by using the <b>Resource Editor</b>; this utility is available for download from EPICweb. Any images contained within this custom file will override images within the base resource file. Typically, the value you enter for this setting is: ".res\MfgCustomImages.resource"</p>
DnsIdentity	<p>Defines the client installation's endpoint identity. The client checks this endpoint identity value against the endpoint authentication returned by the service. When these identity values match, the connection between the client and the endpoint service is validated. This setting helps prevent phishing by stopping the client installation from linking to an endpoint controlled by a malicious service.</p>
DuplicateAttachmentMode	<p>Use this setting to indicate what occurs when two attachments share the same identifier (ID) value. Available options:</p> <ul style="list-style-type: none"> <li>• <b>Prompt</b> - Causes the application to display a window that asks the user to enter a different attachment ID. This is the default option.</li> <li>• <b>AutoDateStamp</b> - Causes the application to automatically add the current date to the end of the attachment ID.</li> </ul>
EnableMultipleDNSEntriesInSANCertificate	<p>If you use .NET 4.6.1 or later with either the <code>UsernameSslChannel</code> or <code>HttpBinaryUsernameSslChannel</code> bindings, you can create certificates that contain additional host names. The .NET system checks the SSL certificate for these additional host names detailed in a Subject Alternate Names (SAN) field. You typically create a SSL certificate in this way to secure multiple sites across different domains. To activate this feature, you change this configuration setting to <b>True</b>.</p>
EnableSslStreamSecurity	<p>Indicates whether you want to activate authentication between the client machine and the Secure Sockets Layer (SSL). To activate this feature, set this configuration setting to <b>True</b>.</p>

XML Tag	Purpose and Expected Value
EndpointBinding	<p>Indicates how this client checks for authentication certificates through Internet Information Services (IIS). When a user logs into the application, the selected method checks whether the user can access the Epicor application. Available options:</p> <ul style="list-style-type: none"> <li>• <b>UsernameWindowsChannel</b> - This NET.TCP binding authenticates transactions through an Epicor Username and Password. Windows checks for existing Epicor user accounts to authenticate logins.</li> <li>• <b>UsernameSSLChannel</b> - This NET.TCP binding authenticates transactions using a Secure Sockets Layer (SSL) X509 certificate. Leverage this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor application.</li> </ul> <p>Selecting this option causes the <b>SSL Certificate Subject Name</b> and <b>DNS Endpoint Identity</b> fields to appear. You use these fields to enter the name of your SSL certificate and the identity of the server.</p> <ul style="list-style-type: none"> <li>• <b>Windows</b> - This NET.TCP binding authenticates transactions using a Windows Username and Password. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.</li> <li>• <b>HttpBinaryUsernameSslChannel</b> - This HTTP binding protocol authenticates using a Secure Sockets Layer (SSL) X509 certificate. The data transfers between the client and server using Hypertext Transfer Protocol (HTTP). Instead of the transport, the message which contains the data transfer is encrypted. Because this binding does not use Hypertext Transfer Protocol Secure (HTTPS), it tends to be slower than bindings which use HTTPS.</li> </ul> <p>Use this method for application servers that handle smart client installations when users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor ERP application.</p> <p>Selecting this option causes the SSL Certificate Subject Name and DNS Endpoint Identity fields to appear. You use these fields to enter the name of your SSL certificate and the identity of the server.</p> <ul style="list-style-type: none"> <li>• <b>HttpsBinaryUsernameChannel</b> - This HTTPS binding authenticates transactions using an Epicor Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). HTTPS encrypts the data transfer.</li> </ul>

XML Tag	Purpose and Expected Value
	<ul style="list-style-type: none"> <li>• <b>HttpsBinaryWindowsChannel</b> - This HTTPS binding authenticates transactions using a Windows Username and Password. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).           <p>You can select this method for application servers that handle smart client installations and Epicor Web Access (EWA) installations where users access the application through the same domain. Any user with a Windows Username and Password within this domain can successfully log into the Epicor application.</p> </li> <li>• <b>HttpsOffloadbinaryUserNameChannel</b> - This HTTPS protocol binding is a configuration that offloads encryption handling to an intermediary Application Request Router such as an F5.           <p>The binding authenticates using an Epicor Username and Password token. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.</p> </li> <li>• <b>HttpsOffloadBinaryAzureChannel</b> - This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an intermediary Application Request Router such as an F5.           <p>The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Azure AD. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.</p> </li> </ul>
	<p> <b>Important</b> When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the <b>AddressFilterModeAny</b> node in web.config as shown below:</p> <pre data-bbox="894 1628 1475 1755">Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens &lt;AddressFilterModeAny /&gt;</pre>
	<ul style="list-style-type: none"> <li>• <b>HttpsOffloadBinaryIdpChannel</b> - This HTTPS protocol binding is a configuration that offloads encryption handling between Epicor ERP to an</li> </ul>

XML Tag	Purpose and Expected Value
	<p>intermediary Application Request Router such as an F5.</p> <p> <b>Important Epicor Identity Provider</b> is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available <b>internally</b> to Epicor.</p>
	<p>The binding authenticates using a security token by specifying a valid authentication claim between Epicor ERP and Epicor Identity Provider deployment. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS). This protocol is configured to move encryption handling to an intermediary Application Request Router like F5 or a similar router.</p> <p> <b>Important</b> When this binding is implemented, in order to avoid the AddressFilter mismatch error, be sure to uncomment the <b>AddressFilterModeAny</b> node in web.config as shown below:</p> <pre data-bbox="894 1058 1475 1178">Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens &lt;AddressFilterModeAny /&gt;</pre> <ul style="list-style-type: none"> <li>• <b>HttpsBinaryAzureChannel</b> - Use this protocol to enable authentication of ERP application users against users in Microsoft Azure Active Directory (Azure AD).       <p>This binding relies upon the user authenticating against Azure Active Directory and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).</p> </li> <li>• <b>HttpsBinaryIdpChannel</b> - Use this protocol to enable authentication of ERP application against Epicor Identity Provider (IdP).</li> </ul> <p> <b>Important Epicor Identity Provider</b> is a new Global Authentication Service that unifies various identity and authentication mechanisms across ERP products. The service will be made available for approved customers in upcoming releases of Epicor ERP. By default, this option is only available <b>internally</b> to Epicor.</p>

XML Tag	Purpose and Expected Value
EnforceApiKeyForRestApiV1	This binding relies upon the user authenticating against IdP and obtaining a token to present to Epicor ERP. The data transfers between the client and server using Hypertext Transfer Protocol Secure (HTTPS).
EnforceApiKeyForRestApiV2	Note the binding you select in the .sysconfig file must match the setting on the application server. You can review and update this application server setting in the <b>Epicor Administration Console</b> . For more information on how you set up each binding option, review either the <b>Epicor 10 Architecture Guide</b> or the <b>System Administration Guide</b> .
EnterpriseSearchURL	Use this setting to enable or disable the requirement of API Keys in all requests against the Epicor ERP REST API version 1. By default, the value of this setting is set to <b>false</b> . If the setting is missing or has an empty value, it is interpreted as <b>false</b> . Set it to <b>true</b> if you wish to make API Key a required parameter.
HelpAboutCopyrightText	Use this setting to enable or disable the requirement of API Keys in all requests against the Epicor ERP REST API version 2. By default, the value of this setting is set to <b>true</b> . If the setting is missing or has an empty value, it is interpreted as <b>true</b> . Set it to <b>false</b> if you wish to make API Key an optional parameter.
HelpAboutCopyrightURL	The Uniform Resource Identifier address the client uses by default to launch the Enterprise Search functionality. When the Enterprise search is launched, it uses the URL you define in this setting value.  You can, however, override this default URL address within each company record; use the Company Configuration- System - General Settings sheet to enter a different URL for the specific company.
	Likewise, you can override the URL value defined on the company on a specific user record. Launch the User Maintenance - List sheet and enter the alternate Enterprise Search URL you want for the current user.  The order of precedence for URL addresses:
	<ol style="list-style-type: none"> <li>1. User record (User Maintenance)</li> <li>2. Company record (Company Configuration)</li> <li>3. Configuration Settings File</li> </ol>
	The <b>copyright text</b> for the About dialog box.
	The <b>copyright URL</b> for the About dialog box.

XML Tag	Purpose and Expected Value
HelpAboutImage	The <b>bitmap file</b> for the Help About window
HelpAboutProductText	The product text for the About dialog box.
HelpAboutTitleText	The title text for the About dialog box.
HHCustomMenuID	<p>The menu ID for the sub process that causes customized Handheld menus to load onto your screen.</p> <p>The client's sysconfig file should be set to the MenuID of the form in Menu Maintenance as follows:</p> <ul style="list-style-type: none"> <li>• <b>&lt;HHCustomMenuID value="HHMN0002" /&gt;</b></li> </ul>
HomePageURL	<p>Displays the <b>Home Page Uniform Resource Locator</b> (URL) that represents the homepage website. If you need to locate this URL, open the *.sysconfig configuration file for your application and locate the HomePageURL node. Typically this file is found in the <b>client &gt; config</b> folder of your Epicor client installation.</p> <p>For example, your HomePage URL may look similar to the following:  <a href="https://qa.americas.epicor.net/ERP102300/Apps/ERP/Home">https://qa.americas.epicor.net/ERP102300/Apps/ERP/Home</a>.</p>
MaxBOMRU	<p>The number of most frequently used business objects whose security settings should be cached when a user logs in.</p> <p>Logic then tracks this number of business objects in the following XML file:</p> <pre>C:\Documents and Settings\All Users\ApplicationData\Epicor\&lt;appserver_and_port&gt;\&lt;version&gt;\&lt;company&gt;\ BOsecMRUList\ BOMRUList_&lt;userID&gt;.xml</pre> <p>This cached information helps minimize the number of calls between client and server, improving performance.</p> <p>This is the default location of the cache folder, but it can change based on the AlternateCacheFolder setting</p>
MaxClssAttrMRU	<p>The number of most frequently used datasets. The information on the tracked datasets is used at login to both fetch (get) and memory cache the extended properties for frequently used datasets.</p> <p>The logic tracks this number of datasets in the following XML file:</p> <pre>C:\Documents and Settings\All Users\ApplicationData\Epicor\&lt;appserver_and_port&gt;\&lt;version&gt;\&lt;company&gt;\ClsAttrMRUList\ ClsAttrMRUList_&lt;userID&gt;.xml</pre>

XML Tag	Purpose and Expected Value
	<p>This cached information helps minimize the number of calls between client and server, improving performance.</p> <p>This path is the default location of the cache folder, but it can change based on the AlternateCacheFolder setting.</p>
MESCustomMenuID	<p>The menu ID for the sub process that allows customized MES menus to be loaded.</p>
MESImage	<p>The default image that is used by the MES menu. The default is blank.</p>
OperationTimeOut	<p>This setting defines how messages are sent and received by this client machine. If a message is not sent or received before this timeout value, the message attempt is stopped. This timeout value also applies when the client sends reply messages for a request/reply service operation and a callback contract method. The default value is 300 (30 seconds).</p>
PredictiveSearchKeyPressDelay	<p>Predictive searches are custom BAQ searches you can attach to a specific field, and they display search results in a floating tooltip window. When a user starts typing in a field linked to a predictive search, this value controls how long it takes for the BAQ linked to the search to run. When you set this option to use a longer delay, the user can enter more text, but the results will take longer to display. The default value is 1500 (1.5 seconds).</p>
PredictiveSearchPopupFadeDelay	<p>When a predictive search runs, this value controls how long the floating tooltip window displays until it fades from view. The default value is 10000 (10 seconds).</p>
ProductBrandIcon	<p>An optional icon that appears on the far right of the application Title Bar.</p>
ProductBrandText	<p>Optional text that appears on the right side of the application Title Bar. If both ProductBrandIcon and ProductBrandText are specified, the text appears to the left of the icon.</p>
ProductLogonImage	<p>An alternate bitmap image that appears in the upper half of the logon dialog box.</p>
ProductID	<p>The product identifier; for example "Epicor".</p>
ResourceFile	<p>A path name to the resource file. This file contains images and other resources that can be changed by partners for branding purposes; for example ".\res\MfgBaselineImages.resources"</p>
SessionManager	<p>The <b>Session Manager</b> tracks all of the instances of the application running on this computer, so that users can</p>

XML Tag	Purpose and Expected Value
	launch several instances <b>without</b> logging in and consuming an additional license. Typically this will just monitor one user, but it can monitor several instances if <b>Terminal Services</b> are enabled. Here are the expected values for this setting:
	<ul style="list-style-type: none"> <li>• <b>ActiveHidden</b> - The default value. This value causes the Session Manager to run, but its icon is not displayed within the <b>System Tray</b>.</li> <li>• <b>ActiveInTray</b> - Causes the Session Manager to run; there is an icon displayed in the Windows system tray.</li> <li>• <b>Disables</b> - Causes the Session Manager to be turned off whenever a shortcut or <b>Information Worker</b> runs.</li> </ul>
	Any Information Worker processes or shortcuts you launch do not consume an additional license if the Session Manager is running and an instance of the client application is already logged on to the appropriate AppServer.
SessionManagerUri	The Uniform Resource Identifier address that the client should use to communicate with the manager service.
SkipHomeUrlValidation	Indicates whether the client application needs to validate its connection to Home Page. If this value is set to True, then no validation occurs. If the Home Page URL is invalid, the user is redirected to an error page instead. This setting helps to troubleshoot login issues.
SysmonPort	The port used for the Session Manager. Enter the port that this computer will use. For example: 7777
TcpKeepAlive	When you activate this setting, you help prevent timeout errors that may occur because of firewall inactivity. The setting does this by sending a data packet once during each time interval. This makes sure the client stays connected to the server.
	The format for this interval setting is <b>HH:MM:SS</b> (Hours:Minutes:Seconds). For example, <TcpKeepAlive value="00:05:00" /> indicates the TCP/IP layer stays active by sending a data packet once every five minutes. By default, this setting is inactive (commented out). To use it, remove the comment (<!-- -->) characters and then enter a time interval. Typically you enter values in the 1 minute to 1 hour range, although you can enter longer time intervals if needed.
ToolbarSettings	The path and XML file that defines the users' default settings for the toolbar functionality. For example, <b>.\res\ToolbarSettings.xml</b>

XML Tag	Purpose and Expected Value
WCFCertValidation	Indicates whether the client application and WCF service need to validate their connection through a certificate. If this value is set to True, a certificate is required for this client installation to communicate with the WCF service.
Version	The current release and patch number for the application; for example 10.1.500.

## User Settings

The User settings contain parameters which only apply to a specific user. Use these parameters to activate the Single Sign On feature, System Monitor settings, login settings, or search settings.

Typically system administrators define these settings for a specific user; this configuration settings file is then used to launch the application on the specific workstation.

XML Tag	Purpose and Expected Value
ActiveFormSettings	<p>In both the Classic and Shell mode, this setting controls the ability to preserve the state of forms when the user logs off (exits) the smart client. Using this control, you can save the information about the forms that are open and records that display. When you log in again, all the saved forms open and load with the appropriate record. Available options:</p> <ul style="list-style-type: none"> <li>• <b>ManualSave</b> - When used, the <b>Save Active Form Shortcuts</b> and <b>Delete Active Form Shortcuts</b> options available in the client. Use these options to manually Save and Delete the active forms data. <ul style="list-style-type: none"> <li>• In the <b>Classic Menu</b> interface, these buttons are found on the <b>Options</b> menu.</li> <li>• In the <b>Modern Home Page</b> interface, these buttons are found on the sliding <b>Context</b> menu at the bottom.</li> <li>• In the <b>Kinetic Home Page</b> interface, these options are found in the <b>Utilities</b> menu in the top right corner of the home page window.</li> </ul> </li> <li>• <b>AutoSave</b> - Open forms and data are automatically saved when the client is closed.</li> <li>• <b>NeverSave</b> - No forms data is saved when the client is closed.</li> </ul>
AutoScaleMode	<p>The concentration of pixels on the window, to accommodate different geometries of forms in different versions of Windows.</p> <ul style="list-style-type: none"> <li>• "<b>None</b>" - The default. No adjustment of forms is done.</li> <li>• "<b>Dpi</b>" - An adjustment (dots per inch) of concentration for pixels is done on forms.</li> </ul> <p>The forms are adjusted to adhere to the DPI field on the <b>Display Properties - Settings - Advanced - General</b> form in Windows.</p> <p>Common settings are 96 DPI and 120 DPI.</p>

XML Tag	Purpose and Expected Value
ContextMenuNestingLevel	<p>Use this setting to adjust the size of the context menus. Depending on the value you enter, context menus can become taller or shorter. Expected values:</p> <ul style="list-style-type: none"> <li>• "<b>0</b>" - All <b>Open With</b> items display within the <b>More...</b> sub-menu.</li> <li>• "<b>-1</b>" - All <b>Open With</b> items are displayed directly on the context menu.</li> <li>• "<b>X</b>" - Substitute an integer (2, 3, 4 and so on) value to indicate how many items will be displayed in the context menu; the remaining items will be displayed in the <b>More ...</b> sub-menu.</li> </ul>
	For example:
<ContextMenuNestingLevel value ="0"/>	
DataCollectionUser	<p>Defines whether or not this user is a <b>data collection user</b>; these users only have access to Data Collection functionality. Only two values can be used - "<b>true</b>" or "<b>false</b>"</p>
DefaultSearchFormLocation	<p>This value controls the default location of search forms as they open. Available options:</p>
	<ul style="list-style-type: none"> <li>• <b>Top</b> - Search forms open at the top of the window from where you launched the search. This value generally provides more real estate for displaying the search results.</li> <li>• <b>Center</b> - Search forms open in the middle of the window from where you launched the Search. This setting is best for Multi-Monitor configured client systems, as the search window opens centered on the user interface form regardless of which monitor is displaying the Epicor application.</li> </ul>
DefaultSearchPageSize	<p>Use this value to control the maximum number of records returned by a search for display within the search results. Lower values generally make more efficient use of server and network resources. Common settings range from 100 to 1000.</p>
EnableVideoHelp	<p>Use this setting to enable links to Epicor Knowledge on Demand videos related to specific ERP programs. Possible values:</p>
	<p><b>True</b> - the default value. Video Help icon displays in the programs that have contextual video help enabled.</p>
	<p><b>False</b> - select this value to disable Video Help. The Video Help icon does not display in the UI.</p>
EOBrowser	<p>The properties of this setting are optional. They can be used by the Epicor Support to diagnose and work around issues with Chromium on different customer environments.</p>
	<ul style="list-style-type: none"> <li>• <b>LogPath</b> - Use this property to specify the path for the console message log file. The default value is "%appdata%\epicor\console.log".</li> <li>• <b>LogEnabled</b> - Set this property to <b>True</b> to enable console message logging. By default, it is set to <b>False</b>.</li> <li>• <b>SharedMemory</b> - Use this property to enable memory sharing by the EO Browser-based Epicor ERP programs and applications - for example, the Kinetic Home Page or the EDD Quick Access Panel. This allows reducing</li> </ul>

XML Tag	Purpose and Expected Value
	<p>consumption of local memory resources on machines running Epicor ERP clients. Possible values:</p>
	<p><b>True</b> - This value enables the memory sharing functionality.</p>
	<p><b>False</b> - Set <b>SharedMemory</b> to <b>False</b> if you don't want ERP programs to share memory.</p>
	 <b>Note</b> If the setting is not present in the configuration settings file, the ERP application behaves as if this setting is set to <b>True</b> .
	<ul style="list-style-type: none"> <li>• <b>DisableGPU</b> - The default value of this property is <b>False</b>. Set it to <b>True</b> to disable GPU for the EOBrowser.</li> <li>• <b>ExtraCommandLines</b> - Use this property to specify additional command line arguments to be passed to the EOBrowser engine.</li> </ul>
	<p>For example, you can set its value to "<b>--disable-databases</b>" to disable HTML 5 DB support. Use space to separate multiple arguments. For example, use "<b>--disable-databases --disable-local-storage</b>" to disable both HTML 5 DB support and local storage support.</p>
	<ul style="list-style-type: none"> <li>• <b>Remote Debug Port</b> - Use this property to specify a port for remote debugging.</li> </ul>
FormOpenMode	<p>Use this setting to determine the initial behavior of a user interface (UI) form as it opens. When no value is specified for this setting, a UI form opens with no special processing.</p>
	<ul style="list-style-type: none"> <li>• <b>AutoSearch</b> - The primary search for each UI form automatically displays as the form launches.</li> <li>• <b>AutoPopulate</b> - The primary search for each UI form is automatically run, and all selected records automatically populate the form as it displays on your screen.</li> </ul>
IgnoreWhiteSpaceOnLabelClick	<p>This setting defines the interface label area affected by click. When set to <b>"false"</b>, indicates that interface elements, for example, fields, check boxes, or radio buttons, are activated when user clicks any part of the label, including blank spaces. You can change this setting to <b>"true"</b> if you want interface elements to be activated only when user clicks the text part of the label.</p>
LastLoginID	<p>This setting is used with the <b>LoginDefault</b> setting.</p> <ul style="list-style-type: none"> <li>• When LoginDefault is set to <b>Last</b>, the value of LastLoginID is the last user ID entered during the logon process.</li> <li>• When LoginDefault is set to <b>List</b>, the value of LastLoginID is a series of previously entered user IDs that have accessed the application.</li> <li>• For the other LoginDefault setting values, LastLoginID is not used and is typically set to have no value.</li> </ul>

XML Tag	Purpose and Expected Value
LaunchType	<p>Use this setting to switch between the Classic Menu and the Modern Shell Menu. Possible values:</p> <ul style="list-style-type: none"> <li>• "<b>MainMenu</b>" - Causes the client installation to launch using the Classic Menu. Users navigate this interface through a tree view that displays nodes for module groups, modules, and programs.</li> <li>• "<b>Shell</b>" - Causes the client installation to launch using the Modern Shell Menu. Users navigate the interface through tile groups that contain related programs.</li> </ul>
LoginDefault	<p>The login default setting that defines what appears in the <b>User Name</b> field. Possible values:</p> <ul style="list-style-type: none"> <li>• "<b>Last</b>" - Displays the last user ID that was used.</li> <li>• "<b>List</b>" - Displays a list of all the recently entered user identifiers.</li> <li>• "<b>Windows</b>" - Displays the same user ID used to log onto Windows on this client machine.</li> <li>• "<b>None</b>" - No default value; the User Name field will be blank.</li> </ul>
Password	<p>The password used for the automatic login (Epicor Account) feature. This encrypted password is generated by the application when a system administrator activates the <b>Single Sign On</b> feature and the current user selects the <b>Automatically sign on</b> check box on the <b>Preferences</b> window.</p> <p>For more information about how to activate this feature, review the <b>Single Sign On (Epicor Accounts)</b> section in the <b>System Administration Guide</b>.</p>
	<p><b>Note</b> This setting is not included in the default Configuration Settings File template. It is automatically added and populated with a value when the <b>Single Sign On</b> feature is activated. It can also be added manually at any time.</p>
SelectTextOnEnter	<p>This setting determines whether an entire word or number is selected when you click in a field with a value.</p> <p>Values are true or false. The default is <b>false</b>.</p>
SetFormToScreenSize	<p>This setting controls the size of Epicor form window at opening. When your screen resolution is 1024 x 768 or smaller, you can set this to "<b>true</b>" to have your Epicor form windows maximized at opening in order to see the whole working area. The default value is "<b>false</b>" which means that windows are normal size when opened.</p>
SingleSignOn	<p>The choices are <b>true</b> or <b>false (the default)</b>. A value of <b>true</b> means that Epicor should use single sign-on logic, and not prompt for user ID and password but instead use the user ID of the current Windows user.</p> <p>Single Sign On is a different login feature that you can also set up for your users. For information on this login feature, review the <b>Single Sign On</b> section later in this guide.</p>

XML Tag	Purpose and Expected Value
SDKUser	<p>Defines whether or not the user is a Software Developer Kit user, with developer tools available. Only two values can be used - " <b>true</b>" or " <b>false</b>"</p> <p>The Software Developer Kit (SDK) is a separate application you can use to create new programs, reports, and processes for Epicor ERP. Use the SDK to develop features unique for your business or locality.</p>
StartSystemMonitor	<p>Defines whether or not the System Monitor will start when the application is launched. Only two values can be used - " <b>true</b>" or " <b>false</b>"</p>
SmtpServer	<p>The location of the smtp server; the smtp server is required for email.</p>
SpLogonMode	<p>Specifies user credentials for attachments linked to a SharePoint library. Available options:</p> <p><b>Default</b> – The SharePoint library uses the current Windows account.</p> <p><b>Interactive</b> – If you set the <b>File Transfer Mode</b> to use the <b>Client System Direct Copy</b> option, use this option to cause the SharePoint logon window to display when users access the attachments. Users enter their account credentials in this window. They can then decide whether the system will save their credentials; to do this, they select the <b>Remember Me</b> check box. This window then no longer displays.</p> <p>For more information, continue reviewing the Implementation User Guide; the Epicor Content Management chapter details how you set up file attachments for specific records.</p>
Style	<p>Use this setting to launch the application with a default theme and option. You can display the application using a look and feel that you prefer. The attributes you define are the style and the options for that specific theme.</p> <p>To use the default Epicor appearance without running the styling features, enter "<b>None</b>" in this setting option. If you use this configuration settings file to launch the <b>Epicor Handheld</b> interface for display on a high resolution device, be sure to set this value to "None". This prevents additional styling from being applied against the fonts on the high resolution device, and the HandHeld interface will display correctly.</p>
	<p>Enter "<b>Default</b>" to use the theme defined as the default on the server. If you would like to use another server distributed theme (other than default), specify its name and file extension. To use a theme from any location on a local computer, enter the complete path and file name.</p>
	<p>For example:</p>
	<pre>&lt;Style value="None"        options="SpecifyName None Default"/&gt;</pre>
	<pre>&lt;Style value="Default"        options="SpecifyName None Default"/&gt;</pre>
	<pre>&lt;Style value="BlueMain.isl"        options="SpecifyName None Default"/&gt;</pre>
	<pre>&lt;Style value="C:\epicor\MyThemes\BlueMain.isl"        options="SpecifyName None Default"/&gt;</pre>

XML Tag	Purpose and Expected Value
SystemMonitorNonPriorityPoll	<p>The frequency that determines how often the client System Monitor checks the server when non-priority print jobs are scanned and processed. This non-priority value is used for Scheduled reports.</p> <p>This value is measured in milliseconds; the minimum value is 3000. The higher this number can be set, the more network traffic is avoided.</p> <p>This value is used with <b>SystemMonitorPriorityPoll</b> and <b>SystemMonitorPriorityPollDuration</b> to determine how the System Monitor interacts with the tasks sent to it.</p>
SystemMonitorPriorityPoll	<p>The frequency that determines how often the client System Monitor checks the server when priority print jobs are scanned and processed. This non-priority value is used for reports sent immediately to the System Monitor.</p> <p>This value is measured in milliseconds; the minimum value is 3000. The higher this number can be set, the more network traffic is avoided.</p> <p>This value is used with <b>SystemMonitorNonPriorityPoll</b> and <b>SystemMonitorPriorityPollDuration</b> to determine how the System Monitor interacts with the tasks sent to it.</p>
SystemMonitorPriorityPollDuration	<p>The value of this setting determines how long the System Monitor will remain in Priority Polling Mode.</p> <p>By default, the System Monitor regularly polls the AppServer using the milliseconds defined for the <b>SystemMonitorNonPriorityPoll</b> value. This <b>Non-Priority Mode</b> is used by the application to process scheduled reports through the System Monitor. When a report is submitted directly (not scheduled) for processing, the System Monitor is then switched to <b>Priority Polling Mode</b>. While in Priority Polling Mode, the System Monitor polls the AppServer using the milliseconds defined for the <b>SystemMonitorPriorityPoll</b> value.</p> <p>The Priority Polling Mode lasts for the milliseconds value you define for this SystemMonitorPriorityPollDuration setting. Once the process goes past this duration value, the System Monitor returns to Non-Priority Polling Mode.</p> <p>This value is used with <b>SystemMonitorNonPriorityPoll</b> and <b>SystemMonitorPriorityPoll</b> to determine how the System Monitor interacts with the tasks sent to it.</p>
UserID	<p>The User Account Identifier required for the automatic login (Epicor Account) feature. This setting is populated by the application when a system administrator activates the <b>Single Sign On</b> feature and the current user selects the <b>Automatically sign on</b> check box on the <b>Preferences</b> window.</p> <p>For more information about how to activate this feature, review the <b>Single Sign On (Epicor Accounts)</b> section in the <b>System Administration Guide</b>.</p> <p> <b>Note</b> This setting is not included in the default Configuration Settings File template. It is automatically added and populated with a value when the <b>Single Sign On</b> feature is activated. It can also be added manually at any time.</p>

XML Tag	Purpose and Expected Value
WrapLabelText	<p>Indicates whether the text on interface labels will wrap to the next line. This setting is useful when you install languages that contain longer strings that need to appear on the interface. Available options:</p> <ul style="list-style-type: none"> <li>• <b>True</b> -- The default value, this setting causes the label text to wrap to the next line on the interface.</li> <li>• <b>False</b> -- Use this option to automatically truncate the label text. The full text value then displays in a tooltip; users hover their mouse over the label to display this tooltip. These tooltips will only appear when the label text is truncated.</li> </ul>

## Deployment Settings

The Deployment settings contain general client distribution parameters.

Modify these parameters to configure how files are moved from the server to the client. These settings define the directory path that the client uses to locate the server files and the method used to receive these files -- either Xcopy or zip.

Typically system administrators define these settings and then distribute the updated configuration files to all workstations within the network for which they apply.

XML Tag	Purpose and Expected Value
clearClientDir	<p>This setting determines whether to clear the local client directory before a client update. Available options:</p> <ul style="list-style-type: none"> <li>• <b>Never</b> - The local client directory is never cleared.</li> <li>• <b>Always</b> - Clears the local client directory if core or custom deployments are updated.</li> <li>• <b>Core</b> - Clears the local client directory if the core deployment is updated. It does not clear the directory if only custom deployments are updated.</li> <li>• <b>Prompt</b> - Asks users if they want to clear the client directory whenever the core or custom deployments are updated.</li> </ul>
clearDNS	<p>This setting determines whether the local client cache will be cleared as part of a client update. Either the default cache location of C:\Documents and Settings\All Users\Application Data\Epicor\&lt;appserver_and_port&gt; or the directory specified by alternateCacheFolder is conditionally cleared based on the value you enter for this setting.</p> <p>Available options:</p> <ul style="list-style-type: none"> <li>• <b>Never</b></li> <li>• <b>Always</b></li> <li>• <b>Prompt</b></li> </ul>

XML Tag	Purpose and Expected Value
DeploymentServer uri	<p>The URI of the deployment directory on the deployment server.</p> <p>Optionally, use the <b>alt_uri</b> attribute to specify the URL of the deployment directory on the fallback deployment server to use for downloading the release client if the primary Deployment Server is not accessible or not available.</p>
deploymentPackage	<p>If the setting of <b>deploymentType</b> is defined as "zip," the value of this setting is the name of the <b>zip</b> file retrieved from the Deployment Server during a client update.</p>
	<p>The default value is: ReleaseClient.zip</p>
deploymentType	<p>Defines the method the deployment system uses to deploy client assemblies (.dll files) to the client. Available options:</p>
	<ul style="list-style-type: none"> <li>• <b>xcopy</b> -- Uses xcopy to deploy the client assemblies into the client installation. These assemblies are then available to launch from the client.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>zip</b> -- Copies a named zip file locally and then unzips the file into the client installation. These assemblies are then available to launch from the client.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>auto</b> -- Only installs the assemblies required to run a specific form the first time a user opens it. When a user first opens a form, the system verifies whether the required .dll files for the form are installed; if some are missing, the .dll files automatically download into the client. It does this by checking both the version number and any deployed customizations. If any version numbers or customizations are different, the updated .dll files download to the client.</li> </ul>
doDateComparison	<p>If deploymentType is set to xcopy, this setting determines whether the xcopy runs and does a date comparison with the /D switch, or downloads all files regardless of date.</p>
	<p>The choices are <b>true</b> (the default) or <b>false</b>. If it is set to false, then xcopy copies all files regardless of modification date.</p>
optimizeAssemblies	<p>A setting that determines whether you can optimize assemblies within the Epicor application. The choices are <b>true</b> or <b>false</b>. A setting of true requires that you have admin rights on the client installation.</p>

## Help Settings

The Help settings configure how the help system is hosted.

You can host the help files locally on a client or centrally through a server. You can also define how the client installation accesses Epicor ePortal and Internet based online technical updates.

Typically system administrators define these settings and then distribute the updated configuration files to all workstations within the network for which they apply. For additional information about how to use these settings, review the **Help System** topics in the application help

XML Tag	Purpose and Expected Value
HelpServer uri	<p>The path name used to point the client machine to the help files. If you want to link the help files to a central server instead of individually on each client, enter the path to the help files location on the server.</p> <p>Note you can leave this setting blank and instead specify the server location in Company Maintenance on the General Settings sheet. Enter the server location in the <b>Epicor Help URL</b> field.</p>
AnnotationsOverrideXSL	<p>The <b>path</b> or <b>file name</b> of the .xslt file; this file lets users print out help annotations. If you want to give users the ability to print out their annotations, enter a path or file name within this property.</p>
courseServer uri	<p>The path name for the embedded courses licensed to your Epicor ERP application. After you install the education courses, enter the path to the course within this parameter; for example: "http://EpicorEducation/EpicorEducation9001/"</p> <p>Note you can leave this setting blank and instead specify the server location in Company Maintenance on the General Settings sheet. Enter the server location in the <b>Education Courses URL</b> field.</p>
E9EducationKeysServer uri	<p>Epicor recommends you create a separate configuration settings file for your training environment and then link this settings file to a unique desktop icon. In this way, the embedded courses are not available within your working environment.</p>
featureSummaryHomePage	<p>If the URL changes for <b>Education Courses License</b> server, this setting indicates the new server location which holds these licenses. Typically this value remains blank. If a new server is required, however, enter the URL path for this setting.</p>
	<p>The web page that is to serve as the home page for the Feature Summary.</p>

XML Tag	Purpose and Expected Value
CustomerCenter product	The product and URL used when the user accesses the Customer Center
OnlineSupport product	The product and URL used when the user accesses online (ePortal) support; for example " <b>Epicor Applications</b> " followed by the URL href = " <a href="http://eportal.epicor.com">http://eportal.epicor.com</a> "

## Sort Settings

 **Important** If you update a client installation, the sortSettings section gets overwritten to match the values defined on the server level configuration file. Typically these settings are defined by the system administrator.

XML Tag	Purpose and Expected Value
Sort Method Default	<p>This value indicates the method that will be used globally to sort strings within the application. The available values are:</p> <ul style="list-style-type: none"> <li>• <b>stringSort</b> – The default value, this sort method does not use any special sort weighting. This causes non-alphanumeric symbols, like hyphens, to be displayed together. This is useful, for example, if your company uses the hyphen in part numbers. Under this logic, the hyphen character has a weight like any other character, so records using this character are sorted together, based on the hyphen's Unicode sequence value.</li> <li>• <b>wordSort</b> – This sort method gives non-alphanumeric Unicode characters (like the hyphen) a reduced sort weight, causing these characters to be sorted among the alphanumeric characters. This reduced sort weight is not based on its Unicode sequence value. Under this logic, "co-op" and "coop" are listed together.</li> </ul> <p>To change the global default value for the application, use the following syntax:</p> <pre data-bbox="861 1558 1475 1634">&lt;stringSort value="default" /&gt;                                 &lt;wordSort value="default" /&gt;</pre>
Sort Method Exceptions	<p>You can also create exceptions to the default sort method by adding additional lines after the default value. You do this by defining the table and column (" <b>TableName.ColumnName</b>" ) that will be sorted using the different method. For example, if your application globally uses the wordSort method, you can enter a new line under the default line (&lt;wordSort value="default" /&gt;) that indicates the stringSort method</p>

XML Tag	Purpose and Expected Value
	<p>that will be used on part numbers. This exception value uses the following syntax:</p> <pre data-bbox="861 312 1279 344">&lt;stringSort value= "Part.PartNum" /&gt;</pre> <p>Each exception line only supports one table/column combination. To apply this logic to multiple table/columns, enter multiple lines:</p> <pre data-bbox="861 466 1383 498">&lt;stringSort value="Part.ParNum" /&gt;</pre> <pre data-bbox="861 519 1465 551">&lt;stringSort value="Customer.CustNum" /&gt;</pre> <p>Continue to enter all the exception lines that you need.</p> <p>If a column has a LIKE value, and the LIKE is one of the columns specified here, the other column will use the same sort method logic as well.</p>

## Alternate Configuration Settings Files

You can create a different configuration settings file and then have a specific workstation launch the application with this alternate file. Use this feature to keep the original file while you experiment with different configurations.

To do this, first create the alternate configuration. You then then activate the **/CONFIG** run time argument for the application icon. Use this argument to define the path that contains the alternate configuration settings file.



**Note** Several run-time arguments are available. For example, use the **/RPT** run-time argument to give the application multiple printer options or the **/MES** run-time argument to cause the application to launch the MES Interface.

## Run Time Arguments

Each workstation can be set up to launch the application in a specific mode. These modes, or **run time arguments**, activate immediately when a user double-clicks on the application's icon.

Several run time arguments are available. For example, you can indicate that the application launches either the Dashboard or the MES interface - instead of the default Main Menu. You can also have the application launch using a different configuration file.

Run time arguments are also useful, for example, when you are customizing programs. Normally during Run Time, you have several favorites groups that autoload their programs into memory. However you cannot customize autoloaded programs. To disable this feature while you are customizing, you use the **/AUTOLOADSUPPRESS** run time argument; this prevents the application from autoloading any programs.

You can also use multiple run time arguments at the same time to further define how the application launches on the workstation.



**Example** You want a workstation to only use the MES interface and you also want it to update to the latest version. For this workstation, you use both the **/MES** and **/UPDATE** run time arguments.

## Enter a Run Time Argument

You add run time arguments to the properties of the application icon.

1. On the desktop for the workstation, right-click on the application's icon.  
A **Context Menu** displays.
2. Select the **Properties** command.  
The application's **Properties** window displays; its **Shortcut** tab is in focus.
3. In the **Target** field, enter a **[Space]** after the target directory path.
4. Now enter a **"/"** or a **"-"**, followed by the run time argument.



**Example** C:\epicor\client\Epicor.exe /UPDATE

C:\epicor\client\Epicor.exe -UPDATE

5. To add another run time argument, repeat steps 3 and 4.



**Example** C:\epicor\client\Epicor.exe /UPDATE /CONFIG=mydefault.sysconfig

C:\epicor\client\Epicor.exe -UPDATE -CONFIG=mydefault.sysconfig

6. Click **OK**.

The next time the client application is launched on this workstation, it uses the run time argument(s) you entered in the Target field.

## Run Time Arguments List

This table lists all the run time arguments available for the application. They display in alphabetical order.

You can enter these arguments in two ways. You can enter the entire argument; for example, /AUTOLOADSUPPRESS. However the application also accepts a shorthand version that only uses the first three characters of the argument, for example, -AUT.

You can activate run time arguments using either the right slash ("/") or the en dash ("-").

 **Tip** New run time arguments may have been added since this documentation was written. Use the /HELP or - HELP run time argument to display the current list.

ARGUMENT	PURPOSE
? or <b>HELP</b>	This mode causes a window to appear that displays all the available run time arguments. Use this mode to get a quick list of the current options.
<b>AUTOLOADSUPPRESS</b>	The autoloading feature causes selected favorite groups to load all their programs into memory; it improves the performance of these programs. However if you customize the application, you need to suppress autoloading. By running this argument, you disable autoloading on this workstation.
<b>BASE</b>	Use this argument to prevent the loading of any verticalizations (industry-specific user interface features), customizations, or personalizations. This option is useful for testing the user interface.

ARGUMENT	PURPOSE
<b>CLASSIC</b>	Use this argument to cause the application to launch using the Classic Main Menu interface. Users navigate this interface through a tree view that displays nodes for module groups, modules, and programs.
<b>CONFIG=&lt;filename&gt;</b>	This argument causes the application to use a different configuration file saved in the same folder as the default.sysconfig file. Enter the name of the file after the equals sign. The next time the application is launched on this workstation, it uses this configuration file. For example:  C:\epicor\<YourClientInstall>\Epicor.exe /CONFIG=mydefault.sysconfig
<b>CRM</b>	This argument causes the application to launch using the CRM user interface. Use this mode to display the application for a user with a CRM user license. This interface displays the modules that include: <ul style="list-style-type: none"> <li>• Customer Relationship Management</li> <li>• Case Management</li> <li>• Quote Management</li> <li>• Configurator Management</li> <li>• ShopVision</li> <li>• Trackers</li> <li>• Status Dashboards</li> </ul>
<b>DB</b>	Use this argument to cause the Dashboard interface to launch - instead of the Main Interface. Use this mode if you only want this user to access a dashboard interface.
<b>HH</b>	This argument causes the application to launch using the Handheld MES Interface. Use this mode to display the application within a handheld device. This interface displays the tools needed to report labor, inventory, and material transactions against jobs.
<b>HHC</b>	Use this argument to launch the Handheld MES Interface in Customization mode. You can then customize this interface as you need. For more information, review the Sub Program Deployment documentation.
<b>MES</b>	This argument causes the application to launch the MES Interface - instead of the Main Interface. Use this mode for workstations being used by the shop floor. This interface displays the tools needed to report labor, inventory, and material transactions against jobs.
<b>MESC</b>	Use this argument to launch the MES Interface in Customization mode. You can then customize this interface as you need. For more information, review the Sub Program Deployment documentation.
<b>MENUID=&lt;Menu ID&gt;</b>	You can limit the programs available on the Menu by including a menu identifier with the config run time argument. To do this, add a run time argument (a slash or dash) followed by the specific Menu ID. You can find the specific menu identifier you need within Menu Maintenance. For example:  C:\epicor\client\Epicor.exe /menuid=CRMN0000   <b>Important</b> The MENUID run time argument only works with the Classic Style interface. It does not restrict menu access in the Modern Shell interface.

ARGUMENT	PURPOSE
<b>RPT</b>	<p>This argument applies only to Crystal Reports. It has no affect when printing SSRS reports.</p> <p>Use this argument to give the application multiple printer options. When active, the application first checks to see if a default printer is selected on a Crystal Report definition. If it is, this printer and its settings are automatically used to print out the report. If a printer is not defined on the report definition, however, the default printer selected on the workstation is used instead.</p> <p>Use this argument when you need a specific printer, like a label printer, to print out a specific report.</p>
<b>SHELL</b>	<p>This argument causes the application to launch using the Modern Shell interface. Users navigate the interface through tile groups that contain related programs.</p>
<b>SKIPCHECK</b>	<p>Use this argument to prevent updates from being automatically installed on this workstation. It stops the client application from checking its version number against the current version on the server.</p> <p>Run this argument to streamline how quickly the application launches on this workstation. By disabling these routines, the application no longer automatically updates each time it is accessed.</p>
<b>TE</b>	<p>This argument causes the application to launch using the Time and Expense user interface. Only modules available through this license display on the main interface. Activate this mode for a user who is licensed to only access these modules.</p>
<b>UPDATE</b>	<p>This argument causes the application to skip checking its version number, but then updates the workstation to the current version available at the server. This forces the client to update - even when the version on the client and the server are the same. Use this argument when you install a patch on the server; this patch then automatically updates on your client installations.</p> <p>You can also use this argument when a problem occurs on a client installation. Adding this argument makes sure that the client installation is using the current version.</p>

## Automatic Schedules

You can create recurring, automatic schedules users can select on reports, processes, and other tasks. When the system clock activates a schedule, all tasks assigned to this automatic schedule run.



**Important** This topic or section describes functionality or uses a process that is only available to on-premise ERP installations.

Each schedule is set up to activate at regular, specific intervals - seconds, minutes, days, weeks, and months. Depending on the task linked to the schedule, this feature could cause a specific report to generate and print, a business activity query to export its data, an executive query to populate with current data, and so on. You use System Agent Maintenance to create the schedules available throughout the Epicor ERP application.

### What Can Be Automated

Many reports and process programs throughout the application have a **Schedule** drop-down list. If a program has this list, you can automate it by choosing one of the schedules defined in the system agent record.

All schedules you create through System Agent Maintenance appear on this Schedule list. To automate the program, first select the **Recurring** check box. This activates the Schedule list. When you select a schedule other than Now, this program is added to the selected schedule's tasks. When the system agent launches the selected schedule, this program runs automatically.

You can automate these types of programs:

- **Processes** - Several processes throughout the application can become tasks, like the **Mobile Connect Server Process**, the **Business Activity Query Export Process**, **Process MRP Process**, and so on.
- **Reports** - Most reports have a Schedule list. All your users can select a schedule for various reports. This report default is linked to each user record, so your users can automate the specific reports they need. When the report is linked to a schedule, it then generates and prints through the system agent. For more information on reports, review the **Report Defaults** topic in the application help.
- **Executive Queries** - You use executive queries to create a cube of data gathered for display on an executive dashboard. You define the cube of data you wish to collect within the **Executive Query** program; for more information, review the Executive Query topics in the application help.

 **Important** In order to launch MRP, Multi-Company logic, or BPM Auto-Printing via **REST** calls, an **AppServer URL** pointing to a **Windows** authentication binding or **Epicor user name/Password** binding must be specified on the **System Agent Maintenance > Detail** sheet. Note this value cannot be set to Azure AD authentication binding.

## Process Sets

You can further refine how tasks automatically generate by assigning them to process sets. Each process set can contain an extensive number of tasks - like reports, processes, and executive queries. You then assign the process set to a schedule. When the process set is activated by the schedule, these tasks automatically run through the sequence you define. You can make process sets available for all companies or a specific company.

## Review Tasks and Reports

To review all the tasks being processed by the system agent, use the **Scheduled Tasks** sheet in the **System Monitor**. Launch this function to keep track of your schedules and the tasks assigned to each of them. You can also use the System Monitor to access reports which have been previewed but not yet printed. You can both display and print out these reports. To do this, use the **Reports** sheet within the System Monitor.

## Create an Automatic Schedule

These steps describe how you add a new schedule to the Epicor ERP application.

1. Navigate to **System Agent Maintenance**.

**Menu Path:** System Setup > System Maintenance > System Agent

 **Important** This program is not available in Epicor Web Access.

2. Click the **Down Arrow** next to the **New** button; select **New Schedule**.

3. Enter a **Description** for the new schedule; for example Weekly - Monday. This indicates the schedule runs once a week each Monday.

This value displays on **Schedule** drop-down lists throughout the application.

4. Use the **Schedule Type** drop-down list to determine how often you want this automatic schedule to activate. Available options:

- a. **Daily** - Select the check boxes for the specific days of the week on which this recurring schedule activates. For example, you could create a daily schedule that runs every Tuesday and Thursday.
  - b. **Hourly** - Select this option to set the schedule to run the tasks every hour.
-  **Important** Use this option if you need the tasks to run every hour exactly. To set up a different time interval, use the **Interval** option.
- c. **Interval** - Defines a schedule shorter than a daily schedule. Enter the hours, minutes, and/or seconds that elapse between each run of this schedule. For example, you could create an Interval schedule that runs every two hours.
  - d. **Weekly** - You first indicate how often the schedule should run, such as every 2 weeks. Then select the day of the week on which the schedule activates. For example, you can create a weekly schedule that activates every two weeks on a Friday.
  - e. **Monthly** - Either indicate this schedule runs on a specific day of the month (for example, Every 15th), or select a recurring week and day in the month it should run (for example, The Last Saturday of the month).
  - f. **Once** - Any tasks assigned to this schedule type only activate for a single run; they activate on the date and time you define in the **Next Run** field. For example, tasks assigned to a Once schedule only run on January 3rd, 2018.
  - g. **Startup** - Tasks assigned to a Startup schedule type immediately activate each time the task agent starts.

5. Now select the date and time on which you want this schedule to activate in the **Next Run** field. You can enter this date directly or click the down arrow to display the **Calendar**.

After the system agent runs this schedule, the Next Run field will later display the next date/time on which this schedule will activate.

 **Tip** However if you select the Weekly schedule type, the next date on which the day of the week falls is calculated and you cannot change this value. For example if you select Friday, the next available Friday might be 5/27/2018. This date displays and you cannot enter or select a different date. You can still change the time on which the schedule activates on this calculated date.

6. To indicate this schedule option is ready to select on all Schedule drop-down lists, select the **Enabled** check box.

7. Click **Save**.

The new schedule is now available throughout the Epicor ERP application.

## Select a Schedule

After you define the schedules, users can select these schedules on specific processes, reports, and executive queries. These items become tasks assigned to the schedule.

Be sure your users select schedules that best fit the production workflow at your organization. Some reports and processes require a large amount of system resources to complete. For these tasks, be sure to attach them to schedules that run at off peak hours during the work day or weekends when database activity is low. This prevents the system from slowing down during more active periods in your work week.

To select a schedule:

1. Launch the report, process, or executive query.

2. Click the **Schedule** drop-down list; the schedules you created in System Agent Maintenance display as options. Select the schedule during which you want this program to generate.
3. Now select the **Recurring** check box. This indicates you want this program to run each time the system agent launches the schedule you selected.
4. To finish linking this program to the schedule, click **Actions > Save Defaults**.  
The values you selected on this window become the default values for the report, process, or executive query.



**Tip** Notice additional options are available from this Actions menu. To restore the program to its original values, select Get Defaults. To clear all the current default values, select Remove Defaults.

When the system clock activates this schedule, this program runs, automatically refreshing and generating data.

## Create a Process Set

Instead of assigning tasks individually to schedules, you can instead group them together through process sets. You can then optionally use the process set to define the order in which these tasks generate.

To use this feature, you first create a process set in Process Set Maintenance. You then add reports, processes, and executive queries to process sets through a toolbar button. You can then return to Process Set Maintenance to define the sequence through which these tasks generate. Lastly, you assign the process set to a recurring schedule.

1. Navigate to **Process Set Maintenance**.

**Menu Path:** System Management > Process Sets > Process Set Maintenance



**Important** This program is not available in Epicor Web Access.

2. Click **New**.

3. Use the **Company** drop-down list to define the company inside which this process set is available. Users within this company can then select this process set. If you are in an Epicor ERP environment, you can create process sets for either all companies or the current company. If you are in an Express or SaaS Standard environment, this drop-down list is read-only and displays the current company.

4. Enter the **Process Set ID**. This value identifies the process set throughout the Epicor ERP application.

5. Enter a **Description** for the process set. This value displays on drop-down lists throughout the application.

6. Select the **Allow Simultaneous Processing of Tasks** check box to cause the process set to asynchronously run and complete its tasks. The tasks are then executed at the same time, improving performance.

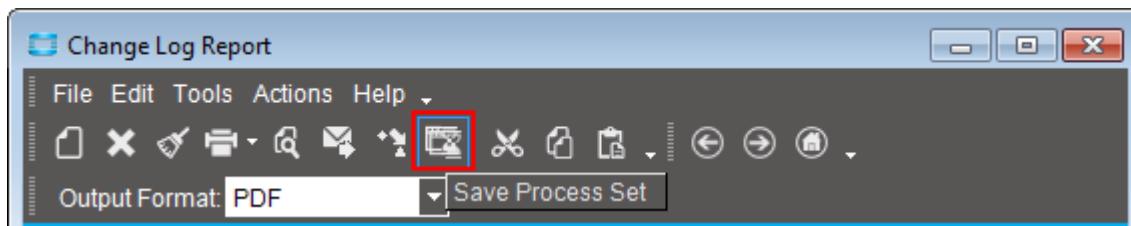


**Tip** Activating this option causes the application to ignore the task sequence defined in the Process Set Tasks grid, so you no longer need to indicate which task must be run before another task.

7. Click **Save**.

8. Now navigate to a report, process, or other task you want to add to this process set.

9. From the program's toolbar, click the **Save Process Set** button.



The **Save To Process Set** window displays.

10. Click the **Process Set** drop-down list and select the process set.
11. Click **OK**.
12. Repeat steps 8-11 to add more tasks to the process set.

## Refine and Schedule a Process Set

You now can determine the order in which tasks generate through the process set. You also assign the process set to a recurring schedule.

1. Return to **Process Set Maintenance**.

**Menu Path:** System Management > Process Sets > Process Set Maintenance



**Important** This program is not available in Epicor Web Access.

2. Click the **Process Set ID...** button to find and select your process set. The task you added to this process set display within the **Process Set Tasks** grid.
  3. If you want to change the sequence through which these tasks run, highlight a task on the grid and click either the **Move Up** or **Move Down** buttons.
  4. Click **Save**.
  5. Now launch **Schedule Process Set**.
- Menu Path:** System Management > Process Sets > Schedule Process Set
6. Select the **Schedule** you want to use for this process set.
  7. Now select the **Recurring** check box to indicate the system agent will automatically launch this process set.
  8. Enter a **User Description** that identifies the purpose for the process set. When you review tasks in the System Monitor, this description displays.
  9. Click **Save**.

## Review Tasks

You use the Tasks sheet in System Agent Maintenance to review the tasks assigned to each schedule.

Each time a schedule activates, all tasks assigned to it run in the order they were assigned to the schedule. This causes selected reports to generate and print, processes to run against current data, business activity queries to

update, and so on. Use the Tasks > Detail and Tasks > List sheets to find out which tasks are assigned to the current schedule and when they were last run. If a task generates an error and does not complete its process, the other tasks on the schedule will continue to run as expected.

### 1. Navigate to **System Agent Maintenance**.

**Menu Path:** System Setup > System Maintenance > System Agent



**Important** This program is not available in Epicor Web Access.

### 2. Use the tree view or the **Schedules > List** sheet to select the schedule you wish to review.

### 3. Click on the **Schedules > Task** sheet.

The **Tasks > List** sheet displays. The **Task List** grid contains the reports, processes, and/or executive queries assigned to the selected recurring schedule.

### 4. To review more details about the task, select its row on the grid.

### 5. Click on the **Tasks > Detail** sheet.

Information on the selected task displays for your review.

## System Monitor

---

Use the System Monitor to verify the processes, reports, and other scheduled tasks you have run.

This program displays tasks scheduled to run within your Epicor ERP application. It displays reports, forms, processes, and other tasks launched by users. Depending on the permissions on your user account, you may see tasks from one or multiple companies. To launch the System Monitor, your user account must have **Allow Session Impersonation** rights; you can then review the tasks for the companies assigned to your user account.

Some organizations group companies together through tenants; if you are a security manager, you can review task activity for companies within your tenant. If you are a global security manager, you can see all tasks for all companies. To do this, click the **Actions** menu and select **Display All Tasks**.



**Important** The options/values for tenant and multi-tenant features are only for Epicor hosted environments. Typically you can ignore these options. Internal Epicor administrators who need more information should refer to the Epicor SaaS Installation Guide.

Use the System Monitor to perform the following tasks:

- **Monitor** - Review the status of the item being run.
- **Preview** - Click the **Print Preview** button to preview a report/form on your screen before it prints. This functionality is only available on the Reports sheet.
- **Print** - Click the **Print** button to print a generated report/form. You can also reprint reports/forms. Use this function to reprint a report (for instance, the Stock Status Report) from a previous date. This functionality is only available on the Reports sheet.

All sheets in the System Monitor display records that indicate a specific program such as a report, executive query, or process (for example, Process MRP) is run. The status of the record determines the sheet where each record displays.

Available sheets:

- **Active Tasks** - This displays the reports, processes, executive queries, or other items currently running.

- **History Tasks** - This displays the reports, processes, executive queries, or other tasks run in the past. Records automatically purge from this sheet when they are 30 or more days old.
- **Scheduled Tasks** - This displays any reports, processes, executive queries, or other tasks scheduled to run in the future.

You can further refine how long items remain on the Reports and History Task sheets by using **Retrieval Properties**. You access these options from the Actions Menu. You determine both the interval type (days, hours, minutes, records) and the length of time these records display on these sheets. This automatically removes older records from the System Monitor, which improves performance and makes it easier to locate the records you need to review.

The System Monitor automatically activates when you start the Epicor ERP application. You can click this program's icon on the system tray on the Windows toolbar to display it. You can also launch this program within the Epicor ERP application.

#### Menu Path

Navigate to this program from the Main Menu:

- System Setup > System Maintenance > System Monitor



**Important** This program is not available in Epicor Web Access.

## Clear Application Cache

When the Epicor ERP application launches on client workstations, a number of items automatically load into memory. As you launch other programs during an Epicor session, some of these programs also are loaded into an application cache to improve performance and track application activity.

These items include dashboards, customizations, and the Customization Maintenance Log.

You can view all of the items currently loaded into your application cache to better understand how the Epicor application is using system resources. If you are troubleshooting a customization, you may also want to clear the items from the application cache to cleanly launch this custom program again without any previous data. This can help you identify performance issues with your customizations.

## Display the Application Cache

Use Windows Explorer to locate the application cache folders. The application cache folders are organized by version and then by company.

To view the application cache for the Epicor ERP application:

1. Launch **Windows Explorer**.
2. Navigate to this path: **C:\Documents and Settings\All Users\Application Data\Epicor\[EpicorInstallationName]\[VersionNumber]\[Company]**
3. Expand the folder for the company you wish to view.
4. Various application cache folders, like **CustomDLLs** and **Customization** display.
5. Expand one of these folders to see the items that have automatically loaded into the application cache.

## Clear the Application Cache

You can remove the items in the application cache at any time.

Use this feature when you need to troubleshoot the performance of a customization or a dashboard. You can then re-launch these programs, potentially improving performance. You will also have cleaner results within the Customization Maintenance Log. You clear the application cache by using an option on the Main Menu.

To remove programs from the application cache:

1. Return to the **Main Menu** of the Epicor application.
2. Click on the **Options** menu.
3. Select **Clear Client Cache**. You will be asked if you want to clear the client cache; click **Yes** on this dialog box.

All items loaded into the application cache are now removed. You can now re-launch these items and review the results within the application cache folders and the Customization Maintenance Log.

## Management Programs

---

The Epicor ERP application contains several programs that help you manage different aspects of your system. Through them you can manage conversions, customizations, file attachments, and so on.

This section of the guide describes each program and where it is located. For more details on each program, review the program's documentation in the application help.

### Conversion Workbench

Use the Conversion Workbench to manage database conversion programs.

Typically security managers can access the Conversion Workbench. However if you are in an Epicor Express or SaaS environment, only global security managers can use the Conversion Workbench. This management program displays on the menu when users log in with their global security manager accounts; other users, including users with security manager rights, cannot access this program.



**Tip** Global security managers can access companies across tenants in an Epicor hosted environment. They can be added to specific companies, regardless of the tenant, to administrate them. This level of security is reserved for Epicor hosted environments such as Epicor Express and SaaS Standard. You assign global security manager rights to users within the Epicor Administration Console. You also use this application to assign global security managers to specific companies.

Data conversions tasks are listed within the workbench's grid and represent standalone processes. You create conversion routines using the Data Conversion Maintenance; you can access this program using the **Actions** menu.

Conversion tasks can be bundled together using Conversion Sets. You typically use this feature when you need to execute a bunch of conversion routines at once. You access Conversion Set Maintenance using the **Actions** menu.

You typically use the Conversion Workbench to do the following:

- **Run mandatory conversions** - The Conversion Workbench is automatically presented on the first login after an upgrade and contains routines a system administrator runs prior to accessing the application.

- **Run custom data conversions** - Use the Conversion Workbench to execute user-run conversion programs, user-prompt maintenance programs and custom conversion sets.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Conversion Workbench



**Important** This program is not available in Epicor Web Access.

## Customization/Personalization Maintenance

Use Customization/Personalization Maintenance to manage the customizations and personalizations that exist within your Epicor ERP application. Its primary feature is the verification functionality which you use to detect problems within customizations or personalizations.

This maintenance program also contains the tools you need to correct issues that occur.

Customization/Personalization Maintenance is especially useful when you upgrade the application to a new version, as it can help you make customized and personalized programs compatible with the current version.



**Tip** When users attempt to launch a customized or personalized program that is not compatible, an error message displays which prevents the user from launching the program. You can then use Customization/Personalization Maintenance to upgrade the program. However if the customized or personalized program is compatible, no error message displays and the user can run the program as expected.

This program has additional functionality for importing and exporting your customizations and personalizations. Leverage these functions to make user modified programs available throughout your organization. You can also use this maintenance tool to delete any customization or personalization. Run this feature when you want to either remove custom program stages you no longer need or remove personalizations made by employees who are no longer with your company.

For System Administrators with **Security Manager** rights, this program can be used to modify fields and delete customizations and personalizations created by users. For System Administrators without Security Manager rights, this program displays in a **Read-Only** format. For more information on security, review the Security documentation.

If you work in a multi-company environment, you can display and update customizations/personalizations in the companies for which you have access. Personalized and customized programs created in the companies defined on your user account within **User Account Security Maintenance** display within this program.

### Menu Path

Navigate to this program from the Main Menu:

- ICE Extend > Operations > Customization Maintenance
- System Management > Upgrade/Mass Regeneration > Customization Maintenance



**Important** This program is not available in Epicor Web Access.

## Dashboard Maintenance

Use Dashboard Maintenance to maintain all dashboards from a central location.

You can run, modify, deploy an individual dashboard, or deploy all your dashboards in Dashboard Maintenance. You can also generate the web form of your dashboards, all from a central location.



**Note** Dashboards can be created using the **Dashboard** application.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Dashboard Maintenance



**Important** This program is not available in Epicor Web Access.

## Data Fix Workbench

Epicor Technical Support periodically releases both database fix scripts and data health scripts that can either check for database issues or correct database corruption.

If you are experiencing database problems, you should import the appropriate data fix script and/or health script into your system. You import these database fix and health (.df) scripts through the Epicor Administration Console by accessing the **Import DB Health(s)** program. Each database fix and health script is created for a specific release and expires after a period of time. If the data fix or health script has expired, return to the Epicor Administration Console and import the current scripts available for your release.

After you import the fix .df scripts, you then run them inside the Epicor ERP application through the **Data Fix Workbench**. Use this program to find and select the database fix script you wish to run. You can then select the database records you wish to update and then run the fix script.

To check on the integrity of database records, you can also use the **Actions** menu to run the **Data Health Check** program. This program runs any database health scripts you imported.



**Important** If you run Epicor ERP in SaaS or a similar hosted environment, only users with Global Security Manager rights can run the Data Fix Workbench.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Data Fix Workbench

## Data Health Check Workbench

Epicor Technical Support periodically releases both database fix scripts and data health scripts that can either check for database issues or correct database corruption.

If you would like to verify the integrity of your database, you should import the appropriate data health script into your system. You import these database health (.df) scripts through the Epicor Administration Console by accessing the **Import DB Health(s)** program. Each health script is created for a specific release and expires after a period of time. If the health script has expired, return to the Epicor Administration Console and import the current scripts available for your release.

After you import the health .df scripts, you then activate them in the Epicor ERP application through the **Data Health Check Workbench**. Use this program to find and select the database health script you wish to run. You then select the database records you wish to validate and run the health script.



**Important** If you run Epicor ERP in SaaS or a similar hosted environment, only users with Global Security Manager rights can run the Data Health Check Workbench.

You can access the Data Health Check Workbench from the **Data Fix Workbench** by launching it from the **Actions** menu. You can also launch this program directly from the Menu.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Data Health Check Workbench

## Data Tag Maintenance

User run Data Tag searches to find and select records grouped together by private or shared tags.

Tags are unstructured text values that provide a way to associate otherwise unrelated records so that you or other users can search for them. For example, you may have a group of customers you want to review on a regular basis. You can create a private data tag for your priority customers called "Priority" and use the Data Tag Search from Customer Maintenance to retrieve all the records at the same time. You might also want to group

a number of sales orders for review by someone else. You can apply a public data tag called "Review" that a sales manager can use from Sales Order Entry.

Private data tags are associated with your user account. Other users cannot retrieve records using your private tags, nor can they see or edit them. Public data tags can be viewed and used in Data Tag Searches by all users. You can add as many data tags as needed to a record, each separated by a space. However because the tags are space delimited, you cannot include a space as part of a data tag.

Use **Data Tag Maintenance** to view and manage the list of data tags added throughout the Epicor ERP application. With this program, you can search for, view, and optionally purge data tags.

**Menu Path:** System Management > Purge/Cleanup Routines > Data Tag Maintenance

## File Attachment Maintenance

If you set up a new file server to store your file attachments, use File Attachment Maintenance to change the base directory path to this file server. Through this program, you update the base path for a group of file attachments that use the same document type, preserving the links your records have to these files.

You first retrieve the current file attachments, either by pulling in all file attachments or filtering them by company and/or document type. You next select a document type and then enter the target base path for the new file server. When you submit the path change, the file attachments update with the new target path. Records linked to these file attachments now use this base path for the selected file attachments.

Note this program only updates the internal directory path to these files. It does not move these files, so you will need to manually place these file attachments in the new base directory on the file server.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Attachment Path Maintenance



**Important** This program is not available in Epicor Web Access.

## Personalization Purge

Use Personalization Purge to remove personalization settings and layers from the system.

Through this program, you first locate all the personalizations created by a specific user. You can then remove a personalization this user no longer wants or remove all personalizations created by this specific user. For example, you might remove all personalizations when an individual leaves your organization.

### Menu Path

Navigate to this program from the Main Menu:

- System Management > Purge/Cleanup Routines > Personalization Purge



**Important** This program is not available in Epicor Web Access.

## Query Conversion Maintenance

Use Query Conversion Maintenance to examine the log of the messages reported during the migration of BAQs from Epicor 9 to Epicor ERP version 10, and to finalize the conversion of external BAQs.

In order to convert external BAQs, the information about field data types must be provided to Epicor ERP version 10. This information is obtained from an external database system and therefore, Epicor ERP server needs to be able to access this system using a valid connection string.

In Epicor 9, external BAQ ODBC connection strings were stored in each BAQ itself. In Epicor ERP 10, this information is maintained under the central location within the External Datasource Maintenance program. Upon the migration from Epicor 9, connection strings are automatically added to list external datasources.

Typically, you use this program to:

- Review any BAQ migration log messages obtained during BAQ migration. You can compare the original and final expression to understand what actions were taken by the migration process.
- Review external datasource connection strings created for all external queries during BAQ migration procedure.
- Verify whether you can connect to external datasources used by external BAQs.
- Run conversion for external BAQs.

**Menu Path:** System Management > Upgrade/Mass Regeneration > BAQ Conversion Maintenance



**Important** This program is not available in Epicor Web Access.

## System Activity Log Purge

Use System Activity Log Purge to delete unwanted system activity log records.



**Important** In **Epicor Cloud ERP - Multi Tenant** or **Epicor Cloud ERP - Dedicated Tenancy**, this program or feature may not be available or may operate under certain restrictions.

To track how users are accessing and updating the database, the application contains the System Activity Log. Use this dashboard to review all the database modifications that occurred within the application. This valuable tool can help you determine where and when specific database changes were carried out and who initiated these changes.

This log is stored on the **Ice.sysactivitylog** table. Since this log tracks database activity, the amount of saved information can cause a database to grow in size very quickly. When you no longer need to review some system activity logs through this dashboard, use the System Activity Log Purge to find, select, and remove specific log files.



**Tip** For more information on this logging program, review the System Activity Log topics later in this guide.

**Menu Path:** System Management > Purge/Cleanup Routines > System Activity Log Purge



**Important** This program may not be available, or operate under certain restrictions in Epicor Cloud ERP.

## Updatable Query Maintenance

Use Updatable Query Maintenance to synchronize your updatable BAQs to become compatible with the current version of the database and software.

Database and software dataset schema changes can occur each time a service pack or a new version is installed on your Epicor application. These changes can cause your updatable business activity queries to become out of sync with the base environment. Your updatable BAQs will then not run. As part of your upgrade process, always be sure to leverage this tool after each release or version is installed on your Epicor application.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Updatable BAQ Maintenance

# Manage Epicor Web Access

Epicor Web Access (EWA) is an alternate Epicor ERP interface that displays through internet browsers. This section of the guide documents some features that will help you better leverage EWA at your organization.

The majority of these items document how you update the web.config file to display features that similarly appear on the smart client. The last part of this section documents how you deploy custom programs and dashboards for use on the EWA interface.

## Clear Cache

You may need to clear the cached browser data for EWA. You do this by first stopping and restarting IIS and then clearing the cache in your internet browser.

This topic describes how you clear the browser cache for the most commonly used internet browsers. To use this information, first follow the steps in the Web Server section. Then follow the instructions for the internet browser you use.

### Web Server

Before you clear the cache on your internet browser, you must first recycle your application pool. To do this:

1. Go to your server machine.
2. Click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
3. Select the **Application Pools** node. The center pane displays the application pools available on your system.
4. Right-click on the application pool for your application server; from the context menu, select **Recycle**.



**Tip** Optionally you can also recycle the application pool within the **Epicor Administration Console**. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The application pool is recycled. Now review the browser cache instructions for the internet browser you use.

### Microsoft Internet Explorer

To clear the Internet Explorer browser cache:

1. Launch **Internet Explorer**.
2. On your keyboard, press the **<F12>** key. A control bar displays at the bottom of the browser window.
3. Click the **Cache** menu.
4. Select the **Clear Browser Cache...** option.

### Microsoft Edge

To clear the Microsoft Edge browser cache

1. Launch **Edge**.
2. Click the **Hub** icon (three horizontal lines at the top bar) and then click the **History** icon.
3. Click **Clear all history**.
4. Select the **Cached data and files** check box.
5. Click the **Clear** button.

### **Mozilla Firefox**

To clear the Mozilla Firefox browser cache:

1. Launch **Mozilla Firefox**.
2. From the toolbar, click **Tools > Options**.
3. The **Options** window displays. Select the **Advanced** tab.
4. Now select the **Network** tab.
5. Locate the **Cached Web Content** group box; click the **Clear Now** button.

### **Google Chrome**

To clear the Google Chrome browser cache:

1. Launch **Google Chrome**.
2. From the toolbar, click the **Chrome** menu.
3. Select the **More Tools...** submenu.
4. Now select the **Clear Browsing Data...** option.
5. The **Clear Browsing Data** window displays. Using the **Obliterate the following items from** drop-down list, select the time interval from which you will remove items. Options include **the past hour**, **the past week**, **the last four weeks**, and **the beginning of time**.
6. Select the check boxes for the types of browsing data you wish to remove.
7. Now click the **Clear browsing data** button.

### **Apple Safari**

To clear the Apple Safari browser cache:

1. Launch **Apple Safari**.
2. Click on **Preferences** menu; select the **Advanced** option.
3. Select the **Show Develop menu in menu bar** check box.
4. The **Develop** menu now displays on the toolbar. Click this menu and select the **Empty Caches** option.

## Configure Crystal Reports

---

If you need to run legacy Crystal Reports in the EWA interface, you can configure EWA so users can print these reports.

You do this by modifying settings in the web.config file:

1. Go to the server machine that hosts **Internet Information Services (IIS)**.
2. Using **Windows® Explorer®**, navigate to your **c:\inetpub\wwwroot\epicorwebaccess** folder. The **web.config** file displays.
3. Open this file in **Notepad** or a similar text editor.
4. Locate the **ReportAppServer** setting.
5. Between the double-quotes (" ") for this setting, enter the name of the server where you installed the Crystal Reports Embedded Server component. Typically this is the same server on which you installed EWA.
6. **Save** the file.
7. **Close** Notepad.
8. Now to complete this process, you must recycle the application pool. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
9. Select the **Application Pools** node.  
The center pane displays the application pools available on your system.
10. Right-click on the application pool for your application server; from the context menu, select **Recycle**.



**Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

Users can now generate Crystal Reports through the EWA interface.

## Configure Embedded Education

---

You can set up EWA so that it displays the Embedded Education button. Users can then launch the Embedded Education courses within the EWA interface.

To do this, you use the same Embedded Education URL setting you have set up for the smart client and your training environments. You entered this URL setting in the .sysconfig files for these environments; this setting is the **CourseServer** setting. You likewise update the web.config file that you use to launch the EWA interface so that it uses this same CourseServer setting. To update the web.config file:

1. Go to the server machine that hosts **Internet Information Services (IIS)**.
2. Using **Windows® Explorer®**, navigate to your **c:\inetpub\wwwroot\epicorwebaccess** folder. The **web.config** file displays.

3. Open this file in **Notepad** or a similar text editor.
4. Locate the **CourseServer** setting.
5. Between the double-quotes (" ") for this setting, enter or paste the **Embedded Education URL** you use for your smart client and training environments.



**Example** http://[YourServerName]/EpicorEducation

6. **Save** the file.
7. **Close** Notepad.
8. Now to complete this process, you must recycle the application pool. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
9. Select the **Application Pools** node.  
The center pane displays the application pools available on your system.
10. Right-click on the application pool for your application server; from the context menu, select **Recycle**.



**Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The application pool is recycled. Now when users log into the EWA interface, the Education button displays. They can click this button to launch the embedded courses.

## Configure Enterprise Search

---

You can set up EWA so that it displays the Enterprise Search button. Users can then launch Enterprise Search from within the EWA interface.

To do this, you use the same Enterprise Search URL setting you have set up for the smart client and your training environments. You entered this URL setting in the .sysconfig files for these environments; this setting is the **EnterpriseSearchURL** setting. You likewise update the web.config file that you use to launch the EWA interface so that it uses this same EnterpriseSearchURL setting. To update the web.config file:

1. Go to the server machine that hosts **Internet Information Services (IIS)**.
2. Using **Windows® Explorer®**, navigate to your **c:\inetpub\wwwroot\epicorwebaccess** folder. The **web.config** file displays.
3. Open this file in **Notepad** or a similar text editor.
4. Locate the **EnterpriseSearchURL** setting.
5. Between the double-quotes (" ") for this setting, enter or paste the **Enterprise Search URL** you use for your smart client and training environments.



**Example** C:\inetpub\wwwroot\EpicorWebAccess

If you installed the EWA site on the same server as Epicor ERP, you enter this path:

\[MyServerName]\epicorwebaccess\

6. **Save** the file.
  7. **Close** Notepad.
  8. Now to complete this process, you must recycle the application pool. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
  9. Select the **Application Pools** node.  
The center pane displays the application pools available on your system.
  10. Right-click on the application pool for your application server; from the context menu, select **Recycle**.
-  **Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The application pool is recycled. Now when users log into the EWA interface, the Enterprise Search button displays. They can click this button to launch Enterprise Search.

## Configure Help

---

You can set up EWA so that users can launch application help through this interface.

To do this, you use the same URL setting you have set up for the smart client and your training environments. You entered this URL setting in the .sysconfig files for these environments; this setting is the **HelpServer** setting. You likewise update the web.config file that you use to launch the EWA interface so that it uses this same HelpServer setting. To update the web.config file:

1. Go to the server machine that hosts **Internet Information Services (IIS)**.
2. Using **Windows® Explorer®**, navigate to your **c:\inetpub\wwwroot\epicorwebaccess** folder. The **web.config** file displays.
3. Open this file in **Notepad** or a similar text editor.
4. Locate the **HelpServer** setting.
5. Between the double-quotes (" ") for this setting, enter or paste the **HelpServer URL** you use for your smart client and training environments.



**Example** `http://[MyServerName]/EpicorHelp`

6. **Save** the file.
7. **Close** Notepad.
8. Now to complete this process, you must recycle the application pool. To do this, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

9. Select the **Application Pools** node.

The center pane displays the application pools available on your system.

10. Right-click on the application pool for your application server; from the context menu, select **Recycle**.



**Tip** Optionally you can also recycle the application pool within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.

The application pool is recycled. Now when users log into the EWA interface, they can display the application help.

## Deploy Customizations

---

You can use Customization/Personalization Maintenance to deploy one or more customizations to the EWA interface. These customizations are then available to use within the EWA interface.



**Important** These customizations must be created using C# code. If you attempt to deploy a customization that uses the older VB code, you will receive errors.

1. Log into **Epicor ERP**.

2. Navigate to **Customization/Personalization Maintenance**.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Customization Maintenance



**Important** This program is not available in Epicor Web Access.

3. Click the **Name** button.

The **Customization/Personalization Search** window displays.

4. Click **Search**.

The customizations available in your Epicor ERP application display.

5. Select the customizations you want to deploy to EWA and click **OK**.

6. You can now generate web form versions of these customizations. Do one of the following:

- a. Deploy a specific customization -- Select a customization from the tree view; now click **Actions > Generate Web Form**.
- b. Deploy all customizations -- Click **Actions > Generate All Web Forms**.

You can now display these customizations within the EWA interface.

## Deploy Dashboards

You can place custom dashboards on the EWA interface. When users next log into the EWA interface, these dashboards appear on the interface.

To do this, you generate the dashboard .dll file and deploy the dashboard as a web form. You then use Menu Maintenance to add this dashboard to the menu.

1. Navigate to the **Dashboard** program.

**Menu Path:** Executive Analysis > Business Activity Management > General Operations > Dashboard



**Important** This program is not available in Epicor Web Access.

2. Activate **Developer Mode**. Click on **Tools > Developer**.



**Note** You can also press **Ctrl + Shift + D** to activate Developer Mode.

3. Click on the **Definition ID** button.

The **Dashboard Search Form** window displays.

4. Click the **Search** button; find and select the dashboard you wish to deploy to the EWA interface and click **OK**.

The dashboard displays.

5. Now click **Tools > Deploy Dashboard**.

The **Deploy Dashboard** window displays.

6. Select the **Deploy Smart Client Application** check box.

7. Now select the **Generate Web Form** check box.

8. Click **Deploy**.

Watch the progress as the dashboard generates. A message indicates when the dashboard successfully deploys. This turns the dashboard definition into a .dll file and deploys this file to the server. It also builds this dashboard as a web form.

9. Click **OK**; exit the **Dashboard** program.

10. You next add this dashboard to the menu. Launch **Menu Maintenance**.

**Menu Path:** System Setup > Security Maintenance > Menu Maintenance



**Important** This program is not available in Epicor Web Access.

11. Use the tree view to find the location on the menu where you want to place the custom dashboard.

12. Click the **Down Arrow** next to the **New** button, select **New Menu**.

13. In the **Menu ID** field, enter **UD** followed by a concise identifier for the dashboard.

14. Enter the **Name** you want for the dashboard.
15. For the **Order Sequence**, enter a value that positions the dashboard on the menu.
16. Now from the **Program** drop-down list, select **Dashboard-Assembly**.
17. From the **Icon** drop-down list, select the **Tracker** option.
18. Now click the **Dashboard** drop-down list; find and select the dashboard you deployed.
19. Click **Save**.
20. Close **Menu Maintenance**.
21. Log out of the Epicor ERP application.

Now when you log into either the smart client application or the EWA application, your dashboard displays in the menu location you defined.

## License Options

---

You can set up EWA to launch through specific licenses. This topic describes how you set up EWA to launch through these licenses.

You activate various licenses by adding the **?LicenseType=** option at the end of the URL address. Then when users log into this web site, this license type activates. The EWA interface displays using the selected license.

Note that you must substitute some values in these listed web site addresses.

- **[YourServerName]** - The name of the server where you installed EWA.
- **[YourSiteName]** - The name you specified during installation for the Epicor Web Access site.

### CRM

The Customer Relationship Management (CRM) license restricts the interface to only display programs related to the CRM module. To restrict EWA to only display CRM programs, enter the following URL:

- **[http://\[YourServerName\]/\[YourSiteName\]/default.aspx?LicenseType=CRM](http://[YourServerName]/[YourSiteName]/default.aspx?LicenseType=CRM)**

### MES

The Manufacturing Execution System (MES) menu displays the interface you typically use on the shop floor. To set up a web site address to display EWA using the MES interface, you enter the following URL:

- **[http://\[YourServerName\]/\[YourSiteName\]/Erp.Menu.MES.MesMenu.aspx](http://[YourServerName]/[YourSiteName]/Erp.Menu.MES.MesMenu.aspx)**

### Time and Expense

The Time and Expense license limits the EWA interface to only display programs related to entering time and expense records. To restrict EWA to only display these Time and Expense programs, enter this URL:

- **[http://\[YourServerName\]/\[YourSiteName\]/default.aspx?LicenseType=TE](http://[YourServerName]/[YourSiteName]/default.aspx?LicenseType=TE)**

# Multiple Environments

Your organization more than likely has multiple Epicor ERP environments used for training, testing, and production. Review this section to learn how to move databases and reports between different environments.

## Self-Signed Certificates - Test Environments

When you use HTTPS, HTTP, or TCP bindings, you commonly use a certificate trusted by both clients and the server to secure communication between these machines.

When the clients exist in the same domain and use a Windows binding, the clients trust the domain and so you do not need a certificate. The domain acts as the certificate. However when either the clients reside on different domains or they do not use a domain, you must implement a certificate. The clients and servers trust this certificate, securing the network communication.

You can purchase certificates from several certificate providers. Microsoft automatically trusts most of these certificates and they display as Trusted Root Certification Authorities in the Certificates MMC console. Microsoft regularly updates these certificates as part of each Windows Update. You can also distribute these certificates through the Group Policy from Active Directory. For your live environment, be sure to secure the system through a trusted certificate.

However for a test environment, you can generate your own certificate and then self-sign it. You then do not need to pay for a certificate. This section describes how you can create a self-signed certificate to secure an internal test environment.

### Determine Setup Process

Depending on which binding you use for your Epicor application, you follow a different setup routine to ensure the security of your network.

If you use a TCP Windows binding, Windows security functions as the certificate and so you do not need to implement a self-signed certificate. For all other bindings, you first create the self-signed certificate and then perform additional setup through either the web.config file or HTTPS. If your system uses WCF, you likewise create a self-signed certificate and then export and import this certificate.

Review the following table to determine whether you need to do the additional **Web.Config Setup Process** or **HTTPS Setup Process**. If you will set up your self-signed certificate in a WCF environment, move on to the **WCF Setup Process** section.

Binding	AppServer URL Schema	Import Public Keys?	Additional Setup
HttpsBinaryUsernameChannel	https://	Yes	HTTPS
HttpsBinaryWindowsChannel	https://	Yes	HTTPS
HttpBinaryUsernameSslChannel	http://	Yes	web.config
HttpsOffloadBinaryUserNameChannel	https://	Yes	HTTPS
TcpCompressedUsernameSslChannel	net.tcp://	Yes	web.config

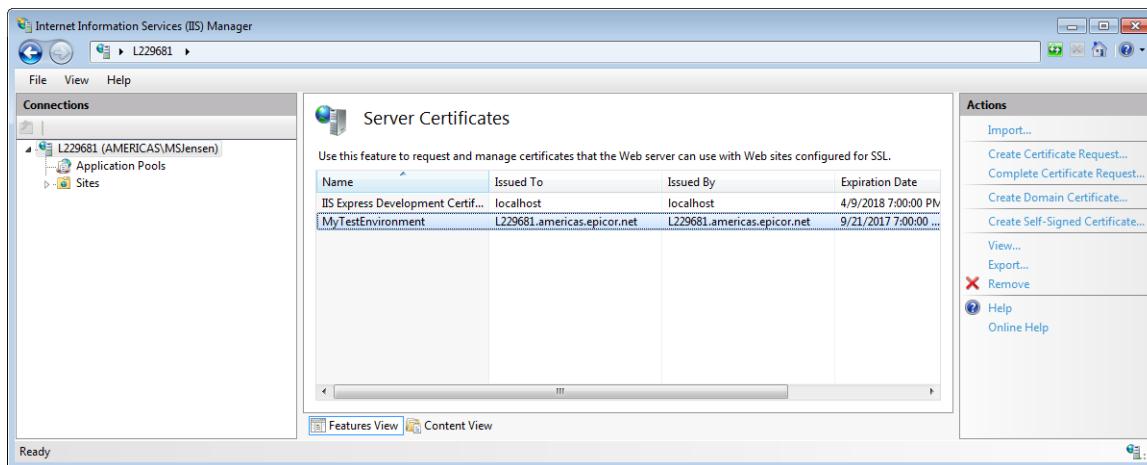
Binding	AppServer URL Schema	Import Public Keys?	Additional Setup
TcpCompressedWindows	net.tcp://	No	None (Uses Windows Security)
TcpCompressedUsernameWindowsChannel	net.tcp://	No	None (Uses Windows Security)
BasicHttp	https://	Yes	HTTPS
SOAPHttp	http://	Yes	web.config

## Create the Certificate

To begin, you first create the certificate.

1. Log into your server machine.
2. Launch **Internet Information Services (IIS) Manager**.
3. Now from the **Connections** pane, select the **[YourFullMachineName]** node.
4. Within the middle pane, select the **Server Certificates** icon.
5. From the **Actions** pane, select **Open Feature**.  
The **Server Certificates** pane displays.
6. From the **Actions** pane, select **Create Self-Signed Certificate**.  
The **Create Self-Signed Certificate** window displays.
7. Enter a **Friendly Name** for the certificate. Enter a name that will help you easily identify the certificate from a list, like MyTestEnvironment.
8. Now from the **Select a certificate store for the new certificate** drop down list, select the **Personal** store option.  
Notice you have two store options -- **Web Hosting** and **Personal**. The Web Hosting store is typically for larger environments that require more than 30 certificates. The Personal store is used for more light weight environments. Because your test environment likely needs less than 30 certificates, you typically select the Personal option.
9. Click **OK**.

Internet Information Services (IIS) creates the certificate. It automatically generates a **Subject Name** which is the same text value as the full machine name (**[YourFullMachineName]**). The Subject Name is sometimes called the **Common Name**. This value links the self-signed certificate with the specific Application Server URL value. Notice both the Friendly Name and the Subject Name display within the IIS window:



The self-signed certificate is now available to use with Internet Information Services.

## Web.Config Setup Process

This section details the setup process to use when your binding requires the certificate be included in the web.config file.

### Update Web.Config File

To begin, you first activate the bindings you will use within the web.config file.

1. Go to your server machine.
2. Using your explorer, navigate to the **C:\inetpub\wwwroot\<YourEpicorInstall>\Server** location.  
The **web.config** file displays.
3. Open this file in **Notepad** or a similar text editor.
4. Locate the **<protocolMapping>** node.
5. Enable the bindings you wish to use by removing the comments that surround the corresponding **<add scheme=>** nodes. You can enable up to three bindings, one for each **NET.TCP**, **HTTP**, and **HTTPS** protocol.
6. Click **Save**.

The web.config file updates with your binding selections.



**Tip** Some bindings require that you enter the certificate in the web.config file. When you enable these bindings and the certificate is not defined in this file, you receive the following error:

- **The service certificate is not provided. Specify a service certificate in ServiceCredentials.**

To correct this error, update the web.config file with the correct protocol and certificate values.

## Export the Certificate - Optional

You now optionally export the self-signed certificate you created so you can then import it into the server's certificate storage. However you only need to import the certificate into storage when necessary; by default Internet Information Services places this certificate in storage.



**Important** When you are using a protocol that requires setup within the web.config file, be sure you export the private key to the certificate. You must export the private key so that the connection between the clients and the server is encrypted.

1. Within the **Internet Information Services (IIS) Manager** window, locate the **Server Certificates** pane. Select the certificate you just created.
2. Now from the **Actions** pane, select the **Export...** option. The **Export Certificate** window displays.
3. Enter a **Export to:** path and file name for the certificate. For example: [DirectoryPath]\[MachineName].pfx
4. Enter a **Password**.
5. Next enter the password again in the **Confirm Password** field. If the passwords match, the OK button activates.
6. Click **OK**.

## Import the Certificate - Optional

You can now import the certificate into the Certificate Store on your server. Remember this process is optional, as Internet Information Services should have already placed your certificate in storage.

1. From your desktop, click **Start > Run**. The **Run** window displays.
2. Enter **mmc** and press **[Enter]**. The **Console** window displays.
3. Click the **File > Add/Remove Snap In...** option. The **Add or Remove Snap-ins** window appears.
4. From the **Available Snap-ins** list, select **Certificates**.
5. Click the **Add >** button. The **Certificate snap-in** window displays.
6. Select the **Computer Account** radio button option.
7. Click **Next**.
8. Select the **Local computer: (the computer this console is running on)** radio button option.
9. Click **Finish**. You return to the **Certificate snap-in** window.
10. Click **OK**.

11. Now from the **Console Root** tree view, expand the **Certificates > Personal > Certificates** node.
12. Right-click the certificate you created (scroll to the side of the grid to display its **Friendly Name**, such as [MachineName].pfx); from the context menu, select **All Tasks > Manage Private Keys**.  
The **Permissions** window displays.
13. Set the permissions to your application server account; the application server can then access the private key. Click the **Add** button.  
The **Select Users, Computers, Service Accounts, or Groups** window displays.
14. Enter the user account set up as the **Application Pool Identity** within the **Internet Information Services (IIS) Manager**. This account is the identity used on the Epicor application pools, and is the same custom account defined on the application server within the **Epicor Administration Console**. After you enter this account, click **OK**.
15. From the list, select the users for whom you want to give access, and then select the **Full Control** check box.
16. Click **OK**.

### Add to Trusted Root Certificates

Because you have created a self-signed certificate, you now must add it to the Trusted Root Certification Authorities on the MMC Console.

1. From the Console Root tree view, expand **Certificates > Trusted Root Certification Authorities > Certificates**.
2. Now in the **More Actions** pane, select the **Certificates > More Actions > All Tasks > Import...** option.  
The **Certificate Import Wizard** displays.
3. Click **Next**.
4. Click the **Browse...** button to find and select the certificate file you just exported. This file uses the Personal Interface Exchange (.pfx) extension.
5. Click **Next**.
6. Enter the **Password** you created for the private key.
7. Click **Next**.
8. Verify you are placing the certificate in the **Trusted Root Certification Authorities** store.
9. Click **Next**.
10. Click **Finish**.
11. A dialog box appears stating that the import process was successful. Click **OK**.
12. Close the **MMC Console**. When asked if you want to save it, click **No**.

## Update the Application Server

To complete the setup for the self-signed certificate for the web.config file, you configure the server to use one of the bindings previously described that require setup in this file.

During the following steps, you update the <serviceCertificate> node.

1. Launch the **Epicor Administration Console**.
2. From the tree view, expand the **Server Management > [YourServer] > [YourApplicationServer]** node.
3. Now from the **Actions** pane, select **Application Server Configuration**.  
The **Application Server Settings** window displays.
4. Navigate to the **Application Server Settings** sheet.
5. Click the **Endpoint Binding** drop-down list, and select the binding option you use.



**Tip** Epicor may add binding options that do not display on this drop-down list. If you do not see the binding option you need on this list, edit the **web.config** file in your server directory so it contains the correct certificate. Within this configuration file, change the `findValue` node to use the name of your certificate:

- If you use a **Personal** store, enter: `<serviceCertificate x509FindType="FindBySubjectName" findValue="[YourCertificateName]" storeLocation="LocalMachine" storeName="My" />`
- If you use a **Web Hosting** store, enter: `<serviceCertificate x509FindType="FindBySubjectName" findValue="[YourCertificateName]" storeLocation="LocalMachine" storeName="Web Hosting" />`

6. Now within the **SSL Certificate Subject Name** field, select the self-signed certificate.
7. Click **Deploy**.

You have completed the steps for setting up the certificate using the web.config file. You can now use the self-signed certificate in your test environment.

## HTTPS Setup Process

This section details the setup process to use when your binding requires that the self-signed certificate be set up using HTTPS.

### Export the Certificate

You first export the self-signed certificate you created on the server machine.



**Important** When you are using a protocol that requires HTTPS setup, only export public key certificates (.cer files). Do not distribute self-signed certificates with private keys (.pfx files) between clients.

1. Return to the **IIS Manager**.
2. From the **[YourServerName]** node, select **Server Certificates**.  
The **Server Certificates** window displays.

3. Now double-click on the certificate.  
The **Certificate** window displays.
4. Click on the **Details** tab.
5. Now click on the **Copy to File...** button.  
The **Certificate Export Wizard** displays.
6. The **Welcome** step displays. Click **Next**.
7. On the **Export Private Key** step, select the **No, do not export the private key** radio button option.
8. Click **Next**.
9. Now on the **Export File Format** step, select the **DER encoded binary X.509 (.CER)** option.
10. The **File to Export** window displays. Click the **Browse...** button to find and select the directory path and the .CER file.
11. Click **Finish**.
12. Click **OK**.
13. Now click **OK** again.  
You return to the **IIS Manager**.

The self-signed certificate (.cer file) is exported to your selected directory file location. Because you are exporting a public key, you do not need to enter a password. Repeat these steps for each server you use in your test environment.



**Important** Because you use an HTTPS binding, the certificate's **Subject Name** must match the **Application Server URL**. If the Subject Name in your certificate is mymachine.mycompany.net, use this name for the application server's URL as well. If this certificate's Subject Name and the Application Server URL do not match, you receive an error message that states:

**Could not establish trust relationship for the SSL/TLS secure channel with authority[AppServerURL You Specified].**

## Import the Certificate

You now import the self-signed certificate from the server into the Local Computer store on the client machines. This creates a secure connection between the client machines and the server in your test environment.

1. From your desktop, click **Start > Run**.  
The **Run** window displays.
2. Enter **mmc** and press **[Enter]**.  
The **Console** window displays.
3. Click **File > Add/Remove Snap-ins**.  
The **Add or Remove Snap-ins** window appears.
4. From the **Available Snap-ins** list, select **Certificates**.
5. Click the **Add >** button.  
The **Certificate snap-in** window displays.

6. Select the **Computer Account** radio button option.
7. Click **Next**.
8. Select the **Local computer: (the computer this console is running on)** radio button option.
9. Click **Finish**.  
You return to the **Certificate snap-in** window.
10. Click **OK**.
11. Now from the **Console Root** tree view, expand the **Certificates > Trusted People** node.
12. On the **Actions** pane, expand **Trusted People > More Actions > All Tasks > Import**.  
The **Certificate Import Wizard** displays.
13. On the **Welcome** step, click **Next**.
14. Now on the **File to Import** step, click the **Browse** button and navigate to the directory location where you exported the certificate. After you select this file, click **Next**.  
The **Certificate Store** step displays.
15. Select the **Trusted People for the Certificate** store and then click **Next**.
16. Now click **Finish** and then click **OK**.
17. Right click the account on the certificate and select **Properties**; verify the **Enable all purposes for this certificate** radio button is selected.

Repeat these steps on each client within your test environment.

### Update .sysconfig Files

You next make sure each client installation uses the correct connection to the server. To do this, update the .sysconfig file used to launch the client.

1. Access a client machine.
2. Using your explorer, navigate to the **config** folder on your client installation. For example: **C:\Epicor \[EpicorVersion]\Client\config**
3. Open the .sysconfig file in a text editor like **Notepad**.
4. Enter the settings in the **<AppServerURL>** and **<EndpointBinding>** nodes. Example settings:
  - If you use **HttpsOffloadBinaryUserNameChannel**, enter

```
<AppServerURL value="https://[YourURL]" />
<EndpointBinding value="HttpsOffloadBinaryUserNameChannel" />
```
  - If you use **HttpsBinaryUserNameChannel**, enter

```
<AppServerURL value="https://[ YourURL]" />
<EndpointBinding value="HttpsBinaryUserNameChannel" />
```
5. **Save** the .sysconfig file.

6. Now launch the Epicor client to verify it displays.

Repeat these steps on each client in your test environment.

## Set Binding

You now set up the binding in the Internet Information Services (IIS) Manager.

1. Return to **Internet Information Services (IIS) Manager**.
2. From the **Connections** pane, expand the **Sites > [YourEpicorWebsite]** node.
3. Within the **Actions** pane, select the **Bindings....** option.  
The **Site Bindings** window displays.
4. If the https binding is available, do the following steps:
  - a. Select the **https** binding.
  - b. Click **Edit**.
  - c. From the **SSL certificate** drop-down list, select your self-signed certificate.
  - d. Click **OK**.
5. If this binding is not available, do the following steps:
  - a. Click **New**.
  - b. Now in the New window, enter these values:

Field	Value
Type:	HTTPS
IP Address:	All Assigned
Port:	443
Host Name:	Friendly Name of Your Self-Signed Certificate
SSL Certificate:	Your Self-Signed Certificate

- c. Click **OK**.

## Update the Application Server

To complete the setup for the self-signed certificate, you configure the server to use one of the HTTPS bindings.

1. Launch the **Epicor Administration Console**.
2. From the tree view, expand the **Server Management > [YourServer] > [YourApplicationServer]** node.
3. Now from the **Actions** pane, select **Application Server Configuration**.  
The **Application Server Settings** window displays.

4. Navigate to the **Application Server Settings** sheet.

5. Click the **Endpoint Binding** drop-down list, and select the binding option you use.



**Tip** Epicor may add binding options that do not display on this drop-down list. If you do not see the binding option you need on this list, edit the **web.config** file in your server directory so it contains the correct certificate. Within this configuration file, change the `findValue` node to use the name of your certificate: `<serviceCertificate x509FindType="FindBySubjectName" findValue="[YourCertificateName]" storeLocation="LocalMachine" storeName="My" />`

6. Within the **SSL Certificate Subject Name** field, select the self-signed certificate.

7. Click **Deploy**.

You can now use the self-signed certificate in your test environment.

## WCF Setup Process

If your environment runs through a binding that does not use the HTTPS protocol, but instead uses its self-signed certificate from WCF services, you set up the certificate through the instructions in this section.

### Export the Certificate

You first export the self-signed certificate you created on the server machine.



**Important** When you are using a protocol that requires HTTPS setup, only export public key certificates (.cer files). Do not distribute self-signed certificates with private keys (.pfx files) between clients.

1. Return to the **IIS Manager**.

2. From the **[YourServerName]** node, select **Server Certificates**.

The **Server Certificates** window displays.

3. Now double-click on the certificate.

The **Certificate** window displays.

4. Click on the **Details** tab.

5. Now click on the **Copy to File...** button.

The **Certificate Export Wizard** displays.

6. The **Welcome** step displays. Click **Next**.

7. On the **Export Private Key** step, select the **No, do not export the private key** radio button option.

8. Click **Next**.

9. Now on the **Export the File Format** step, select the **DER encoded binary X.509 (.CER)** option.

10. The **File to Export** window displays. Click the **Browse...** button to find and select the directory path and the .CER file.

The self-signed certificate (.cer file) is exported to your selected directory file location. Because you are exporting a public key, you do not need to enter a password.

## Import the Certificate

You now import the self-signed certificate from the server into the Local Computer store on the client machines. This creates a secure connection between the client machines and the server in your test environment.

1. From your desktop, click **Start > Run**.  
The **Run** window displays.
2. Enter **mmc** and press **[Enter]**.  
The **Console** window displays.
3. Click **File > Add/Remove Snap-ins**.  
The **Add or Remove Snap-ins** window appears.
4. From the **Available Snap-ins** list, select **Certificates**.
5. Click the **Add >** button.  
The **Certificate snap-in** window displays.
6. Select the **Computer Account** radio button option.
7. Click **Next**.
8. Select the **Local computer: (the computer this console is running on)** radio button option.
9. Click **Finish**.  
You return to the **Certificate snap-in** window.
10. Click **OK**.
11. Now from the **Console Root** tree view, expand the **Trusted Root Certification Authorities > Certificates** node.
12. Right click the self-signed certificate and select **Properties**; verify the **Enable all purposes for this certificate** radio button is selected.

Repeat these steps on each client within your test environment.

## Update .sysconfig Files

You next make sure each client installation uses the correct connection to the server. To do this, update the .sysconfig file used to launch the client so it validates the WCF connection.

1. Access a client machine.
2. Using your explorer, navigate to the **config** folder on your client installation. For example, **C:\Epicor \[EpicorVersion]\Client\config**
3. Open the .sysconfig file in a text editor like **Notepad**.
4. Locate the **<appSettings>** node.

5. Within this node, locate the <WCFCertValidation> node. Set this value to **True**; this indicates the client application and the WCF service must validate their connection through a certificate. A certificate is required for this client installation to communicate with the WCF servier.
6. **Save** the .sysconfig file.
7. Now launch the Epicor client to verify it displays.

Repeat these steps on each client in your test environment.

## Move a Database from Production to Test

---

To properly test a new version or release of the Epicor ERP application, your users will want to run the updated software against current production, distribution, and financial data. Your users can then help determine whether you can update the live environment with the new version or release.

The following topics document how you copy the live database and then use the copy to update the test database.

These instructions assume that the live database and the test database each have a single .mdf and .ldf file. These databases should also both be available within the same Internet Information Services (IIS) instance.

### Stop Test Application Server

You first need to stop the application server in the test environment. While the test application server is stopped, you can then update the test database with the live database.

1. Log into the server machine.
2. Click **Start > Administrative Tools**.  
The **Administrative Tools** window displays.
3. Launch **Internet Information Services (IIS) Manager**.
4. From the tree view, expand the server node.
5. Select the **Application Pools** node.  
The list of application pools display.
6. Right-click on the application pool that runs your test environment; from the context menu, select **Stop**.

The application pool now displays the Stopped status.

### Backup Live Data

You next create a back up file of the live database. This process is similar to the Manual Backup described earlier in this guide.

1. Launch **SQL Server Management Studio**.
2. Within the **Object Explorer**, right-click the database you want to back up, and select the **Tasks > Backup...** option.

The **Back Up Database** window displays. Verify on the tree view that the General sheet displays.

3. From the **Database** drop-down list, select the live database.
4. For the **Backup** type, select the **Full** option. You should always select this option for a manual (or "on-the-fly") backup, as all the data will be recorded in this backup file.
5. Now select the **Copy-only Backup** option. This indicates you are making a separate copy of the database independent from your scheduled, recurring back-ups. You should always select this check box when running a manual backup.



**Important** Recurring full and transaction log backups create a backup chain where each backup builds off the previous backup. If you run a manual or "on-the-fly" backup and do not select this check box, you will interrupt this backup chain. All transactional log backups can only build from this manual full backup, and so you will not be able to restore from any transaction log backups made before this backup.

6. From the **Back up to** drop-down list, select **Disk**.

7. You next identify the **Destination** where the backup database copy will be stored. Notice you can save the backup to either a directory location or a device (if a device is installed). With the **Disk** radio button option selected, click the **Add** button.

The **Select Backup Destination** window displays.

8. Click the **Browse...** button to find and select the directory path. Navigate to the location where you want to save this database backup.

9. You also enter the **Filename** used for the backup. For example, you could enter ERPLiveData.

10. Click **OK** to close the browse window and **OK** again to close the **Select Backup Destination** window. You return to the Back Up Database window.

11. Now click the **Backup Options** node.

12. Enter the **Name** for the backup. This value is important, as it will help you quickly locate the backup file later when you need to restore the database. For example, you could shorten the name to ERPLiveData.

13. Use the **Description** field to enter more information you need about the backup. For example, enter Live Data Backup.

14. Notice the default destination still displays, so you could back up this database in two locations. You only need one backup. Highlight the default option that backs up the file to Microsoft SQL Server; click **Remove**.

15. From the **Set backup compression** drop-down list, select the **Compress backup** option.

By compressing the backup, you improve performance. The backups also take less space on your disk.

16. From the tree view, select the **Media Options** node.

17. In the **Overwrite Media** pane, verify the **Back up to the existing media set** radio button option is selected.

18. Now select the **Overwrite all existing backup sets** radio button option. This reduces the number of backup datasets in the backup disk location.

19. Click **OK**.

Watch the progress bar to check on the backup.

- 20.** When finished, a message displays, indicating the backup was successful. Click **OK**.

The manual backup is now complete.

## Update Test Environment

You now update the test environment with the backup file you created from the live database. This process is similar to what was documented in the Restore a Database topic earlier in this guide.

1. Right-click the test database; from the context menu, select the **Tasks > Restore > Database...** option.

The **Restore Database** window displays.

2. From the tree view, select the **General** node.

3. Select the **Database** radio button option.

4. **Browse** to the directory file location that contains the backup file you just created.

5. Click **OK**.

You return to the Restore Database window.

6. Select the **Restore** check box next to the backup file you want to use to restore.

7. Now on the tree view, highlight the **Options** node.

8. Select the **Overwrite the existing database (WITH REPLACE)** check box.

9. From the **Recovery State** drop-down list, select the **RESTORE WITH RECOVERY** option.

Be sure you select this option. Running the restore in this state causes the database to completely refresh with the data saved in the backup file. The other options restore through different stages.

10. Now from the tree view, click on the **Files** node.

11. Review the directory paths to make sure the test database will be restored.

12. Click **OK**.

The test database is restored (updated) using the options you selected. The test database now contains the most recent data from your live environment.

## Clear Source Values - Optional

Depending on the test environment, you may need to clear some source values from the copied database.

If you are moving the database to a new server or if the database is linked to a file share that no longer exists, you need to clear the **File Root Directory** (FileRootDir). Likewise if you will set up a new task agent, you must clear the data from the **Extended Service Registration** (Ice.ExtServiceRegistration) table.

You clear these source values by running a database query:

1. Within the **SQL Server Management Studio**, click the **New Query** button.

A new query displays in the center pane.

2. Enter the following query:

```
--Removes task agent registration  
delete ice.ExtServiceRegistration  
  
--Removes System agent file directory if it refers to a server not on the n  
etwork  
update ice.SysAgent set FileRootDir = ''
```

3. Now from the **Database** drop-down list, select the test database option.

4. Click **Execute**.

The File Root Directory and the Extended Service Registration table no longer contain source values from the original database. When users access the database and/or you create a new task agent, the database populates with values that match the test environment.

## Start Test Application Server

You are now ready to use the updated database against the Epicor ERP version installed in your test environment. To activate the Epicor ERP application, start the test application server.

1. Return to **Internet Information Services (IIS) Manager**.
2. From the tree view, expand the server node.
3. Select the **Application Pools** node.  
The list of application pools display.
4. Right-click on the application pool that runs your test environment; from the context menu, select **Start**.  
The status for the application pool now displays the **Started** status.
5. Verify the task agent is running for the test application server. Launch the **Epicor Administration Console**.
6. Use the tree view to expand the **Server Management > Server > <Test Application Server Name>** node.  
The Epicor Administration Console connects to the application server. The application server information displays in the center pane.
7. Click the **Task Agent Configuration** button.  
The **Task Agent Service Configuration** window displays. The "Agent Running" message should appear next to a Green icon.
8. If the task agent isn't running, click **Actions > Restart Service...** option.

The task agent now runs. Users can log into the test environment and start using the current data against the programs and processes installed with the Epicor ERP version in the test environment.

## Move Reports Between Environments

After users finishing testing a custom SSRS report, you can then move it from the test environment to the live production environment. Likewise, you may need to move a custom SSRS report from one production environment to make it available in another production environment.

This section of the guide explores how you move reports from one database environment to another database environment. You can move reports between environments using either **Report Style Maintenance** or the **Solution Workbench**. Which program you use depends on how many reports you need to move at the same time. You typically use Report Style Maintenance to move one report. However if you need to move multiple reports at once, use the Solution Workbench.

### Move with Report Style Maintenance

Use Report Style Maintenance to identify the different styles available for printing reports and forms. Through this program, you define the report variations, or styles, available for users to select on report windows.

When you need to move a report from one environment to another, you can use Report Style Maintenance to export the report file out of the source environment to an accessible directory location. You then log into the receiving environment and launch Report Style Maintenance. Use the import feature to pull this report into the receiving environment.

#### Export the Report

To begin, export the report out of the source environment.

Be sure you log in with a user account that has permission to export SSRS reports. You update user accounts in **User Account Security Maintenance**. On the **Options** sheet, verify the **SSRS Report Designer** check box is selected.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

1. Access the source environment.
2. Log into the Epicor ERP smart client application.
3. Launch **Report Style Maintenance**.

**Menu Path:** System Management > Reporting > Report Style



**Important** This program is not available in Epicor Web Access.

4. Click the **Report ID...** button.  
The **Search Form** window displays.
5. Click **Search**.  
The **Search Results** grid populates with the list of available reports.
6. Select the report style you want to export and click **OK**.  
The report record displays in Report Style Maintenance.
7. From the tree view, expand the **[ReportName] > Report Style** node.

8. Select the SSRS style you want to export.
9. Now click **Actions > Download SSRS Report**.  
The **Browse For Folder** window appears.
10. Select a directory location where you want to save the report. Typically you will save this report to the **Desktop**.
11. Click **OK**.

The report .rdl file is saved to the selected directory location.

## Import the Report

You now import the SSRS .rdl file into the receiving environment.

Be sure you log in with a user account that has permission to import SSRS reports. You update user accounts in **User Account Security Maintenance**. On the **Options** sheet, verify the **SSRS Report Designer** check box is selected.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

1. Access the receiving environment.
2. Log into the Epicor ERP smart client application.
3. Launch **Report Style Maintenance**.

**Menu Path:** System Management > Reporting > Report Style



**Important** This program is not available in Epicor Web Access.

4. Click the **Report ID...** button.  
The **Search Form** window displays.
5. Click **Search**.  
The **Search Results** grid populates with the list of available reports.
6. Select the report that uses the style you want to import and click **OK**.  
The report record displays in **Report Style Maintenance**.
7. From the tree view, expand the **[ReportName] > Report Style** node.
8. Select the SSRS style you want to import.
9. Now click **Actions > Upload SSRS Report**.  
The **Browse For Folder** window appears.
10. Select the directory location where you saved the report .rdl file.
11. Next select the .rdl file for the report and click **OK**.

The custom report style uploads to the Reports folder on the server machine. This report style is now available within the receiving environment.

## Move with Solution Workbench

Use the Solution Workbench to create a .cab file which contains objects you wish to bundle together and distribute to other locations within your organization, from one Epicor ERP environment to another environment.

You first create a solution that contains the objects you wish to bundle together, then generate a single .cab file from this solution definition. This single file contains all files and data for the solution and can easily be distributed. Files can include code projects, configuration documents, xml files, and so on, consisting of entire directory structures. Certain files can be 'flagged' so that during installation the user is prompted where those files should be placed on the destination server as the .cab file is installed.

To move reports, you first log into the source environment and launch the Solution Workbench. You then add custom reports to a .cab file. You save this .cab file to a directory location that you can access from the receiving environment. Access the receiving environment and launch the Solution Workbench. You can then install this solution in the receiving environment; the custom SSRS reports are added as part of the install process.

### Create the .CAB File

You begin by creating a solution package (.cab) file in the source environment.

Be sure you log in with a user account that has permission to build solutions and design SSRS reports. You update user accounts in **User Account Security Maintenance**. On the **Options** sheet, verify the **Can Create Solutions** and **SSRS Report Designer** check boxes are selected.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

1. Log into the source environment and the Epicor ERP application.
2. Launch the **Solution Workbench**.

**Menu Path:** System Management > Solution Management > Solution Workbench



**Important** This program is not available in Epicor Web Access.

3. Click the **New** button.
4. In the **Solution** field, enter a name for your .cab file.
5. Now enter a brief **Description** that describes the purpose for the .cab file.
6. Likewise enter any **Internal Notes** you need to further help you identify the contents of the .cab file.
7. Click **Save**.
8. When the **Add New Confirmation** window displays, click **Yes**.
9. Now click the **Add To Solution** button.  
The **Solution Element Search** window displays. Notice the **Element** sheet is active.
10. From the **Available Elements** grid, select the **ReportStyle** option.
11. Click **Search**.  
The **AdvancedElementSearch** window appears.
12. Now click **Search** on this window.  
The **Search Results** grid populates with the reports available in this source environment.

13. Select the SSRS report style(s) you want to export and click **OK**.  
You return to the **Solution Element Search** window.
14. Click the **Add to Solution** button.
15. You are asked if you want to include any dependent files with the solution. Because you are adding a custom report style, you need to add the style's custom report data definition to the solution as well. Click **Yes**.
16. Click **Save**.

## Export the Reports

You next create the .cab file and export it.

1. From the **Actions** menu, select **Build Solution**.  
The **Build Solution** window displays.
2. Select the **Prompt for CAB File Name and Location** check box.
3. Click **Build**.  
The **SSRS RDL Export** window displays.
4. This window asks whether you want to export both the report style and the .rdl file. Click **Yes**.  
The **Save CAB File** window appears.
5. Select a directory location where you want to save the report. Typically you will save this report to the **Desktop**.
6. Click **Save**.  
You return to the **Build Solution** window. The **Build Output** field displays the build progress for the .cab file.
7. When the .cab file is successfully created, click **Close**.

## Import the Reports

You next log into the receiving environment and install the .cab file.

Be sure you log in with a user account that has permission to build solutions and design SSRS reports. You update user accounts in **User Account Security Maintenance**. On the **Options** sheet, verify the **Can Create Solutions** and **SSRS Report Designer** check boxes are selected.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

1. Log into the receiving environment and the Epicor ERP application.
2. Launch the **Solution Workbench**.

**Menu Path:** System Management > Solution Management > Solution Workbench

 **Important** This program is not available in Epicor Web Access.

3. Now click the **Actions** menu and select the **Install Solution** option.  
The **Install Solution** window appears.

4. Click the **Solution File** button.  
The **Open** window displays.
5. Navigate to the directory folder where you saved the .cab file.
6. Select this file and click **Open**.  
You return to the **Install Solution** window.
7. Click **Install**.
8. If you see a **Warning** message that states a duplicate record exists in the receiving database, click **Yes**.  
You return to the **Install Solution** window.
9. The **Installation Output** field displays the progress of the solution installation. When the solution install is finished, click **Close**.

The SSRS reports are now available to run in the receiving environment.

## AFR Integration - Restore Database

---

If you use the Advanced Financial Reporting (AFR) application, you need to complete some additional steps to restore an Epicor ERP database from a backup.

Because Advanced Financial Reporting copies, or replicates, financial data from your Epicor ERP database, you cannot directly restore the database while these AFR replication tasks are active. Instead you must first delete the AFR replication tasks. You can then restore the Epicor ERP database from the backup. After you finish restoring it, you set up the AFR integration again by recreating the AFR replication tasks.

This section of the guide describes how you delete these replication tasks, restore the database, and then recreate these tasks.

### Delete AFR Replication Tasks

You use the AFR Replication monitor to delete AFR replication tasks.

1. Log in to the **AFR Replication Monitor**. To do this, select **Start > Programs > Epicor Software > Advanced Financial Reporting > Replication Monitor**.
2. Click **OK** to connect to the database.
3. On the **Replication Tasks** sheet, select a replication task to remove.
4. Click **Unsubscribe** on the toolbar.
5. When the confirmation message displays, click **Yes**.
6. In the **Task Security** dialog box, specify your **<domain\username>** account.
7. Now in the **Windows account** field, enter your **Password**.
8. Click **OK**.
9. Repeat these steps to unsubscribe all replication tasks.

**10.** Exit the **AFR Replication Monitor**.

The AFR replication tasks are deleted. You can now do maintenance work on this database.

## Restore from Backup

To restore a database from a backup file:

- 1.** On your server machine, launch the **Epicor Administration Console**.
- 2.** Expand the **Server Management** node and select the application server for the database you need to restore.
- 3.** From the **Actions** pane, select the **Stop Application Pool** option.
- 4.** Navigate to the **SQL Server Management Studio**.
- 5.** Right-click the database for which you want to restore the backup, and select the **Tasks > Restore > Database...** option.

The **Restore Database - [YourDatabaseName]** window displays.

- 6.** From the tree view, select the **General** node.
- 7.** Select the **Database** radio button option.  
Notice the **Backup sets to restore** grid displays the path to the manual database backup file you created.
- 8.** Select the **Restore** check box next to the backup name you want to restore.
- 9.** Now on the tree view, highlight the **Options** node.
- 10.** Select the **Overwrite the existing database (WITH REPLACE)** check box.
- 11.** From the **Recovery State** drop-down list, select the **RESTORE WITH RECOVERY** option.  
Be sure you select this option. Running the restore in this state causes the database to completely refresh with the data saved in the backup file. The other options restore through different stages; review the SQL Books documentation for more information on these features.
- 12.** Now from the tree view, click on the **Files** node.
- 13.** Review the directory paths to make sure you will restore the correct database.
- 14.** Click **OK**.  
The database is restored using your selected options.
- 15.** Return to the **Epicor Administration Console**.
- 16.** Verify the application server you stopped is selected.
- 17.** From the **Actions** pane, select **Start Application Pool**.

The database is restored using the selected backup file.

## Recreate AFR Replication Tasks

You next recreate the AFR replication tasks. Your Epicor ERP application will then integrate with the AFR application again.



**Important** When you configure AFR Replication to work with AFR for Excel on a multi-tenant environment, the tenant information replicates from the Epicor ERP database. You only need to configure the AFR Replication when you set up the first tenant. A tenant can have more than one company, but each company code (ID) must be a unique value from other companies that reside in the other tenants. To facilitate this, you should create replication tasks with an option to include all new companies.

Likewise because each user's tenancy is determined by a login account, each user login must also be unique across all tenants. Even though all tenants share the same financial database, users within each tenant cannot view financial data from other tenants.

1. Log in to the **AFR Replication Monitor**. To do this, select **Start > Programs > Epicor Software > Advanced Financial Reporting > Replication Monitor**.

2. Enter the connection details to the SQL Server that hosts the AFR financial database.



**Note** The specified SQL Server account must have the **sysadmin** role in SQL Server which hosts the selected AFR database.

3. Either select an existing AFR database from the **Database** drop-down list or select **Create New** and click **OK** to create a new database.



**Note** If you are migrating a database, the tasks from Epicor 9.05 display in the Replication Monitor grid with the Epicor 9.05 Source ERP type. You may need to delete and re-create these tasks if you want to use new AFR 10 functionality with your database.

4. In AFR Replication Monitor, click the **Subscribe** button.

The **AFR Replication Wizard** displays. The following topics describe how to use this window to recreate your replication tasks.

### Select Database

You begin by selecting the specific database you wish to replicate.

1. In the **Source ERP Type** field, select the database type for the database you will replicate. Typically you select the **Epicor ERP** option.

2. Click **Next**.

3. Now in the **AFR Replication Wizard - From** window, enter the connection for the SQL Server instance that hosts your source ERP application database.



**Note** This SQL Server connection can be different from the server that contains the AFR financial database.

4. From the **Database** drop-down list, select your ERP application database.

5. Click **Next**.

6. In the **AFR Replication Wizard - Company and book filter** window, select the companies and books you want to replicate.

7. Click **Next**.

## Define Tasks

Now define the replication tasks you wish to use.

If you have a large database, you should split the financial data through multiple tasks. If you split tasks by companies, books, or fiscal years, you can re-initialize each task separately in the Replication Monitor. By doing this, you reduce how long it takes to replicate the financial data.

Use the following steps in the AFR Replication Wizard to indicate whether you want to create separate tasks for companies, books, and fiscal years.

1. In the **Re-initialization options** window, indicate how you want to split tasks for books and companies. Available options:

- **All companies together**
- **Each company independently from others**
- **Each company and book independently from others**

2. If you want the companies added to the source database after you create the replication tasks, select the **Include all new companies in replication** check box. When you create replication tasks for a multi-tenant environment, you must select this check box.

3. If you want the books added to the source database after you create the replication tasks, select the **Include all new books in replication** check box.

4. Click **Next**.

5. Now select the tasks you will use for fiscal years. From the **Replicate from year** drop-down list, select the fiscal year from which the replication will start.

6. From the **Re-initialization options** section, select how you want to create tasks for fiscal years. Available options:

- **All years together**
- **Each year independently from others**

7. If you want the fiscal years added to the source database after you create the replication tasks, select the **Include all new years in replication** check box.

8. Click **Next**.

## Aggregation Types

If you selected Epicor ERP as the **Source ERP Type** earlier in the AFR Replication Wizard, you next define how the financial data aggregates during the replication tasks. Use the **AFR Replication Wizard - Type of aggregation** window to define how daily balances aggregate.

1. If you want to aggregate daily balances using the full accounting string from transaction lines, select the **AFR 9.05 behavior** option.
2. If you want to use ERP balance segment settings, select **Aggregate using Balance Segment settings in Epicor ERP**.
3. Click **Next**.

## Miscellaneous Options

You select some final replication options on the **AFR Replication Wizard - Miscellaneous** window.

1. Enter the **Replication task name prefix**. This prefix needs to include the plugin name; for example Epicor ERP.  
When each replication task creates, it uses this prefix followed by a unique numerical identifier. This value is the **Task ID** used by SQL Management Studio for both the **Publisher** and **Subscriber** servers.
2. Notice in the **Select path to shared folder** field, the path to **Snapshot Scripts** folder you created while you installed AFR Replication displays by default. If you need to specify another folder to store replication snapshot scripts, click the **Browse (...)** button to find and select an alternate folder.  
Be sure this Snapshot Scripts folder is available before you initialize the AFR replication tasks. You can store this folder on any workstation in the network, but make sure the Windows account that runs the **Snapshot Agents** has access to this folder. Epicor recommends you share this Snapshot Scripts folder with everyone; this helps avoid security issues.
3. If you want the source database to replicate instantly after you activate these tasks, select the **Start replication immediately** check box.



**Tip** You can also initialize replication later from Replication Monitor.

4. Click **Next**.

## Complete the Tasks

Do the following to complete and activate the AFR replication tasks.

1. In the **AFR Replication Wizard - Task Review** window, review the selected options. You can also change these options.
2. When you are satisfied with these selections, click **Next**.
3. In the **AFR Replication Wizard - Task Security** window, select the **Windows account name** that can create the replication tasks. Make sure this user account has access to both the **SnapshotScripts** functionality and **Snapshots** folders.

**4. Click **Next**.**

The **AFR Replication Wizard - Configuring SQL Replication** window appears. This window displays the progress of the replication tasks.

**5. When the progress bar reaches **100%**, click **Done**.****6. Review the tasks and statuses in Replication Monitor.**

You have now recreated the AFR replication tasks for the current database. For more information on how to create and manage replication tasks, review the Application Help.

# Releases and Updates

---

Epicor periodically makes releases and updates available for your current version of the Epicor ERP application. These releases and updates correct issues and enhance application performance.

You should install these releases and updates when they become available, as they improve how the Epicor ERP application runs and give your users a better experience. This section describes where you can find the installation and migration guides you need to upgrade your current version of the Epicor ERP application.

## Database Migration

---

If you are updating the Epicor ERP application from a 9.05 version to the current 10.x version, you need to migrate your database.

The database migration process updates your 9.05 database to match the database schema for the 10.x database. To migrate your data, use either the **Epicor 10 Migration Guide for SQL** or **Epicor 10 Migration Guide for Progress**. Use the guide that matches your source database.

You download these guides from the EPICWeb site. To access this web site, you must enter your EPICWeb account name and password:

- **Epicor ERP 10.x Documentation** - <https://epicweb.epicor.com/products/epicor-erp-10/documentation>

Expand the node appropriate for your current release (for example, 10.1.400). The deliverables are organized by category; expand the **Installation Guide** category. The SQL and Progress migration guides display below this link.

## Releases

---

Epicor makes service pack releases for the Epicor ERP application approximately every four months. You should always update your application to use the current release, as each one includes important improvements in functionality and performance.

The **Epicor10\_ReleaseUpgradeGuide\_XXXtoYYY** (Where XXX is the previous release and YYY is the current release) describes how to upgrade your existing Epicor ERP application to the current release by installing the new version and performing additional tasks to complete the upgrade.

You can download this guide using the following web site. To access this web site, you must enter your EPICWeb account name and password:

- **Epicor ERP 10.x Documentation** - <https://epicweb.epicor.com/products/epicor-erp-10/documentation>

Expand the node appropriate for your current release (for example, 10.1.400). The deliverables are organized by category; expand the **Installation Guide** category.



**Important** Always install a release in a test environment first. When you are satisfied the release runs as expected, you can then update your live environment.

## Updates

---

Epicor frequently makes updates available for your current release of the Epicor ERP application. Like releases, you should always upgrade your application to use the current update, as each update includes incremental improvements in functionality and performance.

The **Epicor10\_UpdateGuide\_10XXXX** (where 10XXXX is the current update number) describes how to upgrade your existing Epicor ERP application to the current upgrade level by installing it and performing additional tasks to complete the upgrade.

You can download this guide using the following web site. To access this web site, you must enter your EPICWeb account name and password:

- **Epicor ERP 10.x Documentation** - <https://epicweb.epicor.com/products/epicor-erp-10/documentation>

Expand the node appropriate for your update (for example, 10.1.700.3). The deliverables are organized by category; expand the **Installation Guide** category.



**Important** Always install an update in a test environment first. When you are satisfied the update runs as expected, you can then upgrade your live environment.

## Method Changes

---

As part of the development process, changes are occasionally made to the service (business object) methods. You can review these method changes within the Epicor application help.

These method changes typically should not affect your application. However they can sometimes cause Business Process Management (BPM) directives and customizations to no longer run as expected. You should review these method changes and adjust any BPM directives and/or customizations affected by these changes.

For each update and release, Epicor documents these method changes in a spreadsheet. These spreadsheets are included in the application help. As you test a new version, be sure to review this spreadsheet to locate any method changes that may affect your application.

To find these spreadsheets, launch application help. Within the help window, navigate to this location in the **Table of Contents** pane:

- **Epicor ERP 10 Getting Started > Method Changes**

## Schema Changes

---

The database schema is the structure of the tables that make up the Epicor ERP and ICE databases. To implement new features and improve existing functionality, the database schema may change between versions.

These schema changes typically should not affect your application. However these changes may invalidate customizations if they alter the column structure of a table included in a customization. Likewise if you run Business Process Management (BPM) directives that use custom C# code, you may need to update this code to reflect the new database schema.

For each update and release, Epicor documents these schema changes in a spreadsheet. These spreadsheets are included in the application help. As you test a new version, be sure to review this spreadsheet to locate any schema changes that may affect your system.

To find these spreadsheets, launch application help. Within the help window, navigate to this location in the **Table of Contents** pane:

- **Epicor ERP 10 Getting Started > Schema Changes**

## User Interface Changes

---

As part of the development process, changes are occasionally made to the user interface. You can review these user interface changes within the Epicor application help.

These user interface changes typically should not affect your application. However they can sometimes cause Business Process Management (BPM) directives and customizations to no longer run as expected. You should review these user interface changes and adjust any BPM directives and/or customizations affected by these changes.

For each update and release, Epicor documents these user interface changes in a spreadsheet. These spreadsheets are included in the application help. As you test a new version, be sure to review this spreadsheet to locate any user interface changes that may affect your application.

To find these spreadsheets, launch application help. Within the help window, navigate to this location in the **Table of Contents** pane:

- **Epicor ERP 10 Getting Started > User Interface Changes**

# Logging

---

The Epicor ERP application contains many logs you can activate to evaluate nearly every internal process. You can also use client and server logs to identify a specific method or database activity and troubleshoot performance issues.

## Financial Logs

---

This section documents the logs you use to review financial processing in the Epicor ERP application.

### Bank Statement Conversation Log

Use Bank Statement Conversion to convert imported bank statements. This process is necessary when you migrate from the version earlier than Epicor ERP 10.1 and need to use Bank Statement Processing.

It is strongly recommended all bank statements in the obsolete Bank Reconciliation program are posted before you run this conversion process.

The Bank Statement Conversion process will only affect the current company.

#### Log Options

Available logging options:

- **Log Filename** - The default file name is **BankStatementConversion.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

#### Log Location

You launch the Bank Statement Conversion program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > Bank Statement Conversion

### Bulk Address Validation Log

Valid addresses are required for AvaTax® to calculate the correct taxes for your transactions. Use Bulk Address Validation to validate addresses for your companies, sites, warehouses, customers, and customer ship to locations before using Tax Connect in a live/production Epicor environment.

The result of the Bulk Address Validation process is placed inside a .csv file that you can then view with a spreadsheet tool like Microsoft® Excel® or a similar program. You define the location that will store this file within the Log Filename field.

#### Log Options

Available logging options:

- **Log Filename** - Defines the directory path and file name that will be used for the .csv output of this process. Each time this process is run, the results will be placed in this file. You can then view this file within **Microsoft® Excel®** or a similar program. For example: C:/epicor/bulkaddressprocess/BulkAddressValidation.csv

## Log Location

You launch the Bulk Address Validation program from this menu location:

**Menu Path:** Financial Management > Accounts Receivable > General Operations > Bulk Address Validation

## Fix BankTran Reporting Amounts Log

Use the Fix BankTran Reporting Amounts program to recalculate incorrect reporting currency amounts produced by Bank Adjustment errors in Epicor ERP, and restore related data which may be corrupted.

Document and base amounts, and GL Books in base currency, are not affected by this program.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **FixBankTranRptAmounts.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Fix BankTran Reporting Amounts program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > Fix BankTran Reporting Amounts

## Posting Engine Log

The Posting Engine Log tracks the results of your posting rules. You can then evaluate how effective the posting rules are processing transactions.

When the posting engine process runs, the data generated by the posting engine is traced by this log. Each time you run the posting engine process, it adds processing information to the log results. Because of this feature, you can review the history of the posting process. However this log contains a lot of business call details, so only use this log if you understand how to trace the posting results.



**Tip** For more information on how to use this log, review the **Posting Engine Technical Reference Guide**. To find this guide in the application help:

- **General Ledger > Working With > Posting Engine Technical Reference Guide > GL Transaction Type > PE Log Viewer**

The **Troubleshooting** section also contains details on how you use this log.

### Log Options

The following log options are on the **PE Log Viewer**. You access them on the **Settings** sheet:

- **Clear PE File** - Click this button to clear the log results.
- **Show Details** - Select this check box to display all the posting transaction information recorded by the log.
- **Show Warning on Parent** - Select this check box to display posting warnings on parent records.
- **Use Bold Font for Details** - Activate this check box to display the transaction details using a bold font.

## Log Location

You launch the PE Log Viewer program from these programs:

- **GL Transaction Type** - Right click the **Transaction Type** field; from the context menu, select **Open With > PE Log Viewer**.
- **Review Journal** - Right click the **Journal Entry** field; from the context menu, select **Open With > PE Log Viewer**.

## Recalculate Bank Balances Log

Use the Recalculate Bank Balances program to recalculate bank balances based on the transactions that update them.

You may need to run this program when Bank Balances are out of sync with Bank Transactions, Cash Receipts, and Payments. Use this procedure to initiate reconciled balances on migrated bank accounts.

### Log Options

Available logging options:

- **Log Filename** - Enter a file name for the trace log in this field. Once you enter a file name, you can select the **Enable** check box.

### Log Location

You launch the Recalculate Bank Balances program from these menu locations:

**Menu Path:** Financial Management > Accounts Payable > General Operations > Recalculate Bank Balances

**Menu Path:** Financial Management > Accounts Receivable > General Operations > Recalculate Bank Balances

**Menu Path:** Financial Management > Cash Management > General Operations > Recalculate Bank Balances

## Recalculate Customer Credit Log

Use the Recalculate Customer Credit process to easily schedule or run the recalculation of individual or all customer credit data.

You can filter this process by any combination of customer, customer group, or terms code.

### Log Options

Available logging options:

- **Log Filename** - Enter the file name that helps you identify this log. The log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change the directory path.

### Log Location

You launch the Recalculate Customer Credit program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > Recalculate Customer Credit

## Release Data Locked for GL Posting Log

Use Release Data Locked for GL Posting to unlock data locked for GL Posting process. Note, that this conversion process will only affect the current company.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ReleaseLockedData.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Release Data Locked for GL Posting program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > Release Data Locked for GL Posting

## Transfer Balances Log

Use the Transfer Balances Process to transfer balances to the next year.

The Transfer Balances Process can be scheduled. After balances are transferred the first time, they update with each posted transaction or can be re-transferred at any time. This allows you to transfer balances to the next year before current year-end and to have next year opening balance early drafts. Then, you can transfer the final balances after all the previous year adjustments are complete.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **TransferBalances.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Transfer Balances program from this menu location:

**Menu Path:** Financial Management > General Ledger > General Operations > Transfer Opening Balances to Next Year

## UD Codes Creation for Intrastat Log

Use the UD Codes Creation for Intrastat process to automatically populate new user-code tables with the Intrastat information from the FOB, Ship Via, Country, and Company setup tables.

This conversion process is useful if you have already entered your own Intrastat codes into the application and you need validation of Intrastat codes.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **IntrastatUDCodesCreation.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the UD Codes Creation for Intrastat program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > UD codes creation for Intrastat

## Unlock Bank Statement Log

Use Unlock Bank Statement to unlock bank statements for the current company that are locked.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **BankStatementUnlock.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Unlock Bank Statement program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > Unlock Bank Statement

## Unlock Batch Log

Use Unlock Batch to normally process error cash receipt and payment batches.

When you work with batches in Cash Receipt Entry, Cash Receipt Batch Maintenance, AP Payment Entry, or Payment Batch Maintenance, some of these batches may be locked due to some errors. On this occasion you are able to unlock such batches in the Unlock Batch program.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **BankBatchUnlock.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Unlock Batch program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Finance > Unlock Batch

## Use Tax Calculation Log

Use the Use Tax Calculation Process to send posted accounts payable invoice information to Epicor Tax Connect.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **UseTaxProcessLog.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Use Tax Calculation Process from this menu location:

**Menu Path:** Financial Management > Accounts Payable > General Operations > Use Tax Calculation

## Verify Balance Records Log

Use the Verify Balance Records Process to verify that your balance records are accurate. This is done by recalculating the balance from the transaction details and comparing them to the existing balance records.

You can also use the Verify Balance Records Process to rebuild balance records if they become inaccurate, or if the balance setup changes. After determining your selection criteria and executing the program, a report is created that records the results.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **GLVerifyBalances.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Transfer Balances program from this menu location:

**Menu Path:** Financial Management > General Ledger > General Operations > Verify Balances

## Integration Logs

---

Various processes integrate the Epicor ERP application with outside applications such as Epicor Commerce Connect and Product Life Management. Use these logs to review the transactions that generate through these integrations.

## ECC Customer/Consumer Synchronization Log

Use ECC Customer/Consumer Synchronization to synchronize customer, consumer and currency master file data between Epicor Commerce Connect and Epicor ERP.

ECC Customer/Consumer Synchronization synchronizes this data between the specified Epicor ERP company, the ECC Admin Panel and Customer/Consumer Connect ECC sites. It uses the company ID you specify in the External Company ID field in External Company Maintenance to determine the synchronization company that is paired with the ECC Customer external system record defined in External System Maintenance.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ECCCustomerMaster.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the ECC Customer/Consumer Synchronization program from this menu location:

**Menu Path:** System Setup > Commerce Connect > ECC Customer/Consumer Synchronization

## ECC Supplier Synchronization Log

Use ECC Supplier Synchronization to synchronize supplier master file data between Epicor Commerce Connect and Epicor ERP.

ECC Supplier Synchronization synchronizes this data between the specified Epicor ERP company, the ECC Admin Panel and Customer/Consumer Connect ECC sites. It uses the company ID you specify in the External Company ID field in External Company Maintenance to determine the synchronization company that is paired with the ECC Supplier external system record defined in External System Maintenance.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ECCSupplierSync.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the ECC Supplier Synchronization program from this menu location:

**Menu Path:** System Setup > Commerce Connect > ECC Supplier Synchronization

## Export to Mattec Log

Use the Export to Mattec process to export CSV files from the Epicor ERP to Epicor Mattec MES. The Epicor ERP application exports in bulk (folder) rather than individual CSV files. Users can then import and display these manufacturing records in the Mattec interface.

Click the Export Folder button to search for and select the name and directory of the file you want to export. You also specify a Cutoff Horizon Date. Any manufacturing records created before this date are not included in the exported file.

While you run this process, a log generates. Use this log to review any errors that occurred during the export. You can then use this information to correct issues with these records and then run the Export to Mattec Process again.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ExportToMattec\_Error.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Export to Mattec Process from this menu location:

**Menu Path:** Production Management > Engineering > General Operations > Export to Mattec

## Generic Integration Log

Use the Generic Integration Server Process to transform financial information that was imported into the system from outside resources into Epicor records. The appropriate validation and financial calculations are made and the data is returned to the Epicor application (for example, as AR invoices).

Running the Generic Integration Server Process converts the data in the IM tables (IMInv for AR and IMAPInv for AP) to actual tables through the following three actions:

- Translation (static mapping)
- Validation (same validation as Invoice Entry)
- Transformation

This is a step in the overall process of automating the import, creation, and posting of invoices when used in conjunction with the Generic Import Process which imports financial data into the system. Use this functionality to take advantage of the improved performance that processing multiple invoice groups concurrently provides. If this option is not used, invoices are created without tax calculation.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **GenericIntegration.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Generic Integration Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > Generic Integration Server Process

## Generic Import Log

Use the Generic Import Process to import XML data with AR or AP information, with minimal validation, into the Epicor application. This process can be scheduled and multiple processes can run simultaneously.

The XML file must contain mandatory fields to be validated. Refer to the AR Import File Template or AP Import File Template topics for a list that shows the required fields.

After importing AR and AP data, use the Generic Integration Server Process to create standard invoices. You can then post them as a group in AR or AP Invoice Entry.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **GenericImport.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Generic Import Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > Generic Import Process

## PLM Log

Use the PLM Server Process to transfer Product LifeCycle Management integration data from the Manufacturing system to a PLM system.



**Important** In **Epicor Cloud ERP - Multi Tenant** or **Epicor Cloud ERP - Dedicated Tenancy**, this program or feature may not be available or may operate under certain restrictions.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **PLM.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the PLM Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > PLM Server Process



**Important** This program may not be available, or operate under certain restrictions in Epicor Cloud ERP.

## Manufacturing/Distribution Logs

Manufacturing and distributing tasks generate job suggestions, manufacturing schedules, and material requirements. The logs described in this section record the transactions generated by these production processes.

### Auto Job Closing Log

Use the Auto Job Closing Process to automatically close jobs. Any jobs that fall within the thresholds defined on closing codes used in the Epicor application are automatically closed. Any jobs that fall outside these thresholds fail to close.

The log for this process will list each job with its criteria set and status. Jobs that did not close will display the Material, Operation, and Subcontract threshold percentage that caused the failure. For example:

```
Job 01002045 - Criteria Set A100 - Closed
Job 01002051 - Criteria Set C200 - Failed      Asm Seq 0 - Opr Seq 50 - Qty 57%
Job 01002051 - Criteria Set C200 - Failed      Asm Seq 0 - Mtl Seq 20 - Cost 140
%
```

You can then open this job to correct the failure and then manually close the job through the Job Completion/Close Maintenance program.

### Log Options

Available logging options:

- **Log Filename** - Defines the name of the audit log file this process will create. This log file will be saved within the Mfgsysdata/reports directory on your system's application server. After the Job Closing Process is run, you can then review this file to see which jobs did and did not close.

## Log Location

You launch the Auto Job Closing Process from this menu location:

**Menu Path:** Production Management > Job Management > General Operations > Auto Job Closing Process

## Auto Job Completion Log

Use the Auto Job Completion Process to automatically complete jobs. A job that falls within the thresholds defined on completion codes is automatically completed. A job that falls outside these thresholds fails to complete.

The log that generates from this process will list each job with its criteria set and status. Jobs that did not complete will display the Material, Operation, and Subcontract threshold percentage that caused the failure. For example:

```
Job 01002045 - Criteria Set A100 - Completed
Job 01002051 - Criteria Set C200 - Failed      Asm Seq 0 - Opr Seq 50 - Qty 57%
Job 01002051 - Criteria Set C200 - Failed      Asm Seq 0 - Mtl Seq 20 - Cost 140
%
```

You can then open this job to correct the failure and then manually complete the job through the Job Completion/Close Maintenance program.

## Log Options

Available logging options:

- **Log Filename** - Defines the name of the audit log file this process will create. This log file will be saved within the Mfgsysdata/reports directory on your system's application server. After the Job Completion Process is run, you can then review this file to see which jobs did and did not close.

## Log Location

You launch the Auto Job Completion Process from this menu location:

**Menu Path:** Production Management > Job Management > General Operations > Auto Job Completion Process

## Auto Job Firm Log

Use Auto Job Firm Process to automatically separate Plan as Assembly sub assemblies into a new job when the primary job is firmed up.

When a firm job is selected for processing, the Epicor application checks for Plan as Assembly items. When stock is available, the application creates a material record for the subassembly part and designates the due date. The application uses the original job number, plus the assembly number with a demand link to stock based on the MRP parameters.

## Log Options

Available logging options:

- **Log Filename** - The default file name is **AutoJobFirm.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Auto Job Firm Process from this menu location:

**Menu Path:** Production Management > Job Management > General Operations > Auto Job Firm Process

## Auto Job Release Log

Use Auto Job Release Process to automatically release Jobs to the Floor for processing.

You can run Auto Job Release manually, or schedule this process to run automatically. You can also attach the process to a schedule to allow the production planner to automatically release jobs to the floor.

### Log Options

Available logging options:

- **Log Filename** - Use this field to enter a unique name for your processing. It generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change this directory path.

### Log Locations

You launch the Auto Job Release Process program from these menu locations:

**Menu Path:** Production Management > Job Management > General Operations > Auto Job Release

## Backflush Labor Log

You run the Backflush Labor Server Process to backflush all labor placed against current jobs at once. This process only backflushes labor for the current company, and it only uses labor entries marked as Approved.

The process automatically generates a log when you report labor in Time and Expense Entry against a job operation or material marked as Backflush. You can then analyze transactions for Backflush operations and materials.

The log uses a default filename **BackFlushLaborProcess.txt** and includes the following information:

### Backflush Operations

- Company
- Labor Header Sequence
- Labor Detail Sequence
- Assembly Sequence
- Operation Sequence
- Job Number

### Backflush Part Transactions

- Part Transaction Type
- Employee ID
- Material Sequence
- Part Number
- Warehouse
- Warehouse Bin
- Transaction Quantity
- Start /End Dates and Times



### Example

```
11:22:18 Backflush Labor Server Process - Started
11:22:18 Backflush Labor Server Process - Processing
11:22:19 Processing Company: EPIC06 LaborHedSeq: 122585 LaborDtlSeq: 242778
```

```

0 JobNum: 2421 AssemblySeq 0 OperationSeq 20
11:22:19 -----> Backflush Factor 1
11:22:19 -----> Labor Production Created For B Operation: Company:EPIC06 La
borDtlSeq: 2427781 Job: 2421/0/10
11:22:19 -----> PartTran Created TranType STK-MTL EmpID MtlSeq 20 Pa
rtNum lot1 Whse CHI Bin 00-00-00 TranQty 10 EA
11:22:19 -----> Deferred Update executed for updating PartBin CHI/00-
00-00 LotNum Qty 10 EA
11:22:19 Backflush Labor Server Process - Completed
11:22:19 Backflush Labor Server Process - Stopped

```

## Log Options

Available logging options:

- The log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** location. If you need, you can change both the directory path and the file name.

## Log Locations

You launch the Backflush Labor Server Process from these menu locations:

**Menu Path:** Material Management > Inventory Management > General Operations > Backflush Labor Server Process

**Menu Path:** Production Management > Job Management > General Operations > Backflush Labor Server Process

## Calculate Global Scheduling Order Log

Use the Calculate Global Scheduling Order Process window to calculate and assign the order of the jobs for Global Scheduling.

This process will use scheduling on all jobs eligible for Global Scheduling to determine the date from the global schedule start date to get days late.

The new date, along with priority, will be used to determine the scheduling order.

## Log Options

Available logging options:

- Log Filename** - Defines the name of the scheduling log file this process will create. This log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\**.
- Log Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - Basic** -- The log displays the Start Date and Start Time with the number of schedulers (processors) that were run. The log also displays when each processor finished - and if any errors occurred during the process.
  - Process** -- This log displays the Basic information described above. It also includes a log for each scheduler (processor) which displays the jobs that were scheduled.
  - Process and Scheduling** -- This log displays the Basic and Process information described above. It also includes a detail log that displays how each operation was scheduled, including constrained materials and the finite capacity used against each resource.

## Log Location

You launch the Calculate Global Scheduling Order Process from this menu location:

**Menu Path:** Production Management > Scheduling > General Operations > Calculate Global Scheduling Order

## Convert PclnValues Log

Use the Convert PclnValues process to run your saved input values history (PclnValue table) conversion in batches, if you use Configurator and want to migrate from the Epicor ERP version 9 to the Epicor ERP version 10.

You use the Convert Pcln log to evaluate the performance of the Conversion process, troubleshoot errors, and review the progress of a specific Conversion process run.

### Log Options

Available logging options:

- **Log Filename** - Use this field to enter a unique name for your processing. It generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change this directory path.

### Log Locations

You launch the Convert PclnValues program from these menu locations:

#### Menu Path

Navigate to this program from the Main Menu:

- System Management > Rebuild Processes > Mfg / Distribution > Convert PclnValues

## Detect Redundant BOMs Log

Use the **Detect Redundant BOMs** process to run a report that identifies which manufactured parts in your database have circular references in their bill of materials (BOMs). You can then fix these circular references.

A circular reference in a BOM should not typically occur, as a validation in the application prevents this situation from occurring in new BOMs. However redundancies may exist in BOMs created before the validation was added to the Epicor ERP application. Use this process to find and correct these older BOMs.

### Log Options

Available logging options:

- **Include Alternate Methods for Detection** - Determines whether the process examines alternate manufacturing methods for redundant BOMs.
- **Log Filename** - This log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Locations

You launch the Detect Redundant BOMs Process from this menu location:

#### Menu Path

Navigate to this program from the Main Menu:

- System Management > Rebuild Processes > Mfg / Distribution > Detect Redundant Boms

## Global Scheduling Log

Use the Global Scheduling Process to reschedule all your open, engineered jobs.

This program uses the scheduling priority code assigned to each job to determine which jobs should be scheduled before other jobs. All the jobs selected by the Calculate Global Scheduling Order process are placed within the schedule, either on the actual schedule or on a What-If schedule.

### Log Options

Available logging options:

- **Log Filename** - Defines the name of the scheduling log file this process will create. This log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\**.
- **Log Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - **Basic** -- The log will display the Start Date and Start Time with the number of schedulers (processors) that were run. The log displays when each processor finished and if any errors occurred during the process.
  - **Process** -- This log displays the Basic information described above. It also includes a log for each scheduler that displays the jobs that were scheduled.
  - **Process and Scheduling** -- This log displays the Basic and Process information described above. It also includes a detail log that displays how each operation was scheduled, including constrained materials and the finite capacity used against each resource.

### Log Location

You launch the Global Scheduling Process from this menu location:

**Menu Path:** Production Management > Scheduling > General Operations > Global Scheduling

## Import Labor / Scheduling Parameters Log

Use the Import Labor/Scheduling Parameters Process to import labor records or invoke job scheduling from a valid CSV file.

The process reads records from all CSV files found in a designated External MES Input Folder, configured for a Site. If the import line begins with L/P/E/S, all valid records are written in a database as LaborHed/LaborDtl/LaborPart/LaborEquip/SerialNo. If the import line begins SCH, job scheduling is run.

Note: All import lines that fail validations are written to a subdirectory (\Output) under the Input Folder, and display the output filename as OriginalFileName + \_Error.txt.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ImportLaborSched\_Error.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Regenerate Configurations Process from this menu location:

**Menu Path:** Production Management > Scheduling > General Operations > Import Labor / Scheduling Params Process

**Menu Path:** Production Management > Job Management > General Operations > Import Labor / Scheduling Params Process

**Menu Path:** Service Management > Time Management > General Operations > Import Labor / Scheduling Params Process

## Manufacturing Lead Time Calculation Log

Use Manufacturing Lead Time Calculation to enable manufacturing lead time calculations for a single part, product group, site, or for all parts.

Manufacturing lead time is the total lead time required to produce or manufacture all levels of an assembly. Usually this is calculated by system based BOM & Routing. If not calculated, this time can be also manually assigned.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **MfgLeadTimeCalc.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Manufacturing Lead Time Calculation program from this menu location:

**Menu Path:** Production Management > Engineering > General Operations > Mfg Lead Time Calculation

## Material Requirements Planning (MRP) Log

Process MRP is the Material Requirements Planning (MRP) generation process.

The MRP Process examines the demand from forecasts, the master production schedule (MPS), and sales orders. It then compares demand to the current supply from both jobs and purchase orders. When the supply does not meet the demand, it creates new jobs, manufacturing suggestions for existing jobs, and suggestions for purchase orders.

You use MRP logs to evaluate the performance of MRP, troubleshoot errors, and review the progress of a specific MRP processing run. If MRP processing takes up a significant amount of system resources, the entries in these logs can help determine exactly when these processing bottlenecks occur. Likewise, when MRP encounters an error, the log records this error against the processor identifier (PID) and part records that generated it. The MRP log can also help you determine how many processors and schedulers you can make available to maximize MRP performance.

### Log Options

Available logging options:

- **Log** - Use this field to enter a unique name for your processing and scheduling logs. While the MRP Process runs, it uses this text value as a prefix for all the logs you generate. You can then more easily locate these log files, which generate for the company in the **Mfgsysdata/Reports** directory.
- **Logging Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - The **Basic** logging level only displays MRP parameters information.
  - The **MRP** logging level records MRP part processing details information.

- The **MRP and Scheduling** logging level generates additional scheduling logs that document unfirm jobs. Typically you should select this option, as you will track the most information about each MRP process run.
- **Number of MRP Processes** - The Number of MRP Processes modifier defines how many separate threads your server runs to complete the MRP process. This feature improves performance, as you can split one large MRP process into several threads. The process then takes less time to complete. Use this value together with the Number of Schedulers value to maximize the performance of MRP processing and scheduling.
- **Number of Schedulers** - The Number of Schedulers modifier defines how many separate threads your server runs to schedule unfirm jobs. This feature improves performance, as you can schedule unfirm jobs on several threads and the process takes less time to complete. Use this value together with the Number of MRP Processes value to maximize the performance of both MRP processing and scheduling.

## Process Performance

The more processors and schedulers your system can handle, the better system performance you achieve. However if you run the MRP process against too many processors and schedulers, you can also slow down performance or even time out the process. The following section, **Balancing Processors and Schedulers**, describes how you use these two fields with the logs and your server hardware to determine optimal MRP performance.

You should run tests to determine what is the ideal number of threads you can run at the same time. To review these performance times, use the MRP log. You can set this log to run at the Basic level to see the overall time it takes to run the MRP process. If you want more details in the log, select the MRP level to see how long it takes to run each MRP process thread by Load Level and part, or select MRP and Scheduling to review both the MRP process and scheduler threads through separate logs. You can also use the Performance Monitor (PerfMon) to see if a CPU or the disks are causing a performance bottleneck.

Keep in mind that more threads are not always better. As you run your tests, start with a small value to get a base time. Then increase the Number of MRP Processes and/or Number of Schedulers values for each test. Be sure you always make these changes in small increments. Your performance should improve each run, but you will get to a point where it starts to run slower again. This indicates that your server cannot handle any more MRP process or scheduling threads, and you need to reduce the MRP process threads and scheduling threads back to the point where you achieved optimal performance.

If you notice times in the log where the MRP process threads are idle, these processor threads can also be used as scheduling threads. By increasing the number of schedulers, you can then improve the performance of the MRP processors as well.

## Log Location

You launch the Process MRP program from this menu location:

**Menu Path:** Production Management > Material Requirements Planning > General Operations > Process MRP

## MRP Processor Log Organization

Each MRP processor log is organized in five major sections.

The first section records the overall information for the specific processor run. It displays the date/time, defines the processor identifier (PID), and assigns the session number. For example:

Thursday January 5 17:20:19 2012

```
17:20:19 MRP net change process 4 begin - Ver 103 Run Date 01/05/12.  
17:20:19 PID: 6844; Session: 10.2.1.45::ERP10APP1::2012R::1629aac094019ecb:-25:
```

```
134aa75718a:-4b0d
17:20:19 -----
```

The next section details the parameters selected on the MRP Process window. These selections determine how the MRP process generates the results. These various options are documented in the Modifiers section found earlier in this guide. An example section:

```
17:20:19 Cut Off Date          -> 06/30/12
17:20:19 Schedule Start Date  -> 01/05/12
17:20:19 Run Finite Scheduling -> yes
17:20:19 Ignore Constrained Materials -> no
17:20:19 Allow Historical Dates -> no
17:20:19 Use Production Preparation Buffer -> yes
17:20:19 Sort Level 0 MRP Jobs by Date -> no
17:20:19 Recycle MRP Jobs      -> yes
17:20:19 site List             -> EPICOR01
17:20:19 -----
```

The third section documents the process control customizations (if any) you run during the MRP process. You can create C# assemblies that customize MRP to better match your production flow and improve MRP performance. You then set up process control queues to determine the sequence these .p customizations run. For example:

```
17:20:19 -----
17:20:19 Process Control Queue
17:20:19   Group -> Delete; Queue -> DeleteAllPO; Type -> Default; Finite -> no
17:20:19   Group -> Delete; Queue -> DeleteJob; Type -> Job; Finite -> no
17:20:19   Group -> Delete; Queue -> DeleteTO; Type -> TO; Finite -> no
17:20:19     Check List -> DeleteAllPO~DeleteJob~DeleteTO; Last Group -> no
17:20:19   Group -> Load; Queue -> SaveLoad; Type -> Job; Finite -> no
17:20:19     Check List -> SaveLoad; Last Group -> yes
```



**Tip** For more information on this feature, review the **MRP Code Customization** topics in the MRP Technical Reference Guide.

Because the information in these top three sections is often the same, you typically ignore this information. Instead, the fourth section in the MRP processor log contains the processing details you need. This log section generates if you select the **MRP** or **MRP and Scheduling** log levels on the Process MRP window. It records how long it took each MRP part to process, as well as the various records generated through the MRP process.

This section of the log begins by evaluating the parts by **Load Level**. Load Level 0 indicates the part is used/manufactured during the top assembly on each active Bill of Material (BOM). MRP then works through each subsequent assembly in the part BOMs, including all the parts used at this level. The Load Levels go as deep as needed to evaluate each BOM, so the levels that display on the log depend on how complex the BOMs are for each manufactured part. You can use Notepad's Find window to locate when each Load Level runs. By recording the Start Time for each Part Level, you can determine how long it takes MRP to process each level, identifying the busiest Load Levels.

The log then details the processing run against each part included in the load level. The log first defines the site in which the part is manufactured or purchased. It then documents the MRP parameters used with the part, such as Receive Time, Delta In, Delta Out, and so on. The log then displays the unfirm jobs and suggestions MRP deletes before processing new unfirm jobs, stock transactions, purchase suggestions, and other part processing details. When MRP finishes the part's processing, the Done with Part text displays on the log entries. An example part process:

```
17:20:34 Starting Part Level: 0. Wait Time 00:00:14, Parts 0, Jobs 0
17:20:34 Processing Part:005-0005-0112. V103
17:20:34 Processing Part:005-0005-0112 site:EPICOR01.
17:20:34 Parameters: Receive Time -> 1; Planning Fence -> 0; Delta In -> 0; Delta Out -> 0
17:20:34 Deleting suggestions
17:20:34 Deleting unfirm jobs for part 005-0005-0112
17:20:34 Deleting unfirm job MRP00000025613
17:20:39 Deleting unfirm job MRP00000025614
17:20:45 Deleting unfirm job MRP00000025615
```

```

17:20:49 Deleting unfirm job MRP00000025616
17:20:55 Deleting unfirm job MRP00000025617
17:21:01 Processing non-stock transactions for Part:005-0005-0112.
17:21:01 Processing stock transactions for Part:005-0005-0112.
17:21:01 Refresh Forecast for 005-0005-0112 on EPICOR01
17:21:01 Beginning Balance 0
17:21:01 Date changed, process date ?
17:21:01 Date changed, process date 02/04/12
17:21:01 Below re-order, expedite jobs.
17:21:01 Expedite-jobs - qty needs to be expedited:2
17:21:01 Expedite-jobs - Total requirement: 2
17:21:01 Total quantity expedited:0.
17:21:01 Get Destination
17:21:01 Create Intersite Supply
17:21:01 Creating new unfirm job:MRP00000030326 Quantity:2.
17:21:01 Adding to job:MRP00000030326 Quantity:2.
17:21:01 Copying BOM from Part:005-0005-0112 Rev:A3 to Job:MRP00000030326.
17:21:12 Sent job MRP00000030326 to SchedJobI
17:21:13 Date changed, process date 03/04/12
17:21:13 Below re-order, expedite jobs.
17:21:13 Expedite-jobs - qty needs to be expedited:2
17:21:13 Expedite-jobs - Total requirement: 2
17:21:13 Total quantity expedited:0.
17:21:13 Get Destination
17:21:13 Create Intersite Supply
17:21:41 Done with Part 005-0005-0112

```

Notice the start times recorded for each part processing transaction. You can measure how long it takes to process each part by subtracting the first start time from the last start time.

The final section on a MRP Processor log contains the total **Wait/Scheduling** times, which indicates how long this processor was idle while the scheduler placed unfirm jobs on the schedule. This section also contains the Number of Parts, New Jobs, the Reused Jobs, the Deleted Jobs, the Scheduled Jobs, and the Saved Load. For example:

```

23:12:39 MRP process 4 done.  Total Wait/Scheduling Time = 00:14:10
23:12:39 Parts: 1015; New Jobs: 1083; Reused Jobs: 97; Deleted Jobs: 1111; Sche
duled Jobs: 266; Saved Load: 645

```

## MRP Scheduler Log Organization

Each MRP scheduler log is organized in the same way as the MRP processor logs.

The first three sections display similar information as the processor logs – documenting the overall session, MRP process parameters, and process control parameters. The main difference is the MRP process parameters contain the scheduling options selected on the MRP Process window. These options are documented in the Modifiers section found earlier in this guide:

```

17:20:19 -----
17:20:19 Cut Off Date          -> 06/30/12
17:20:19 Schedule Start Date   -> 01/05/12
17:20:19 Run Finite Scheduling  -> yes
17:20:19 Ignore Constrained Materials -> no
17:20:19 Allow Historical Dates -> no
17:20:19 Use Production Preparation Buffer -> yes

```

The fourth section then details the scheduling times for unfirm jobs generated during the scheduler run. This log section generates if you select the MRP and Scheduling log level on the Process MRP window. You can use this section of the log to identify any unfirm jobs which took longer to generate, why certain unfirm jobs will be late, and locate any scheduling errors. For example:

```

17:24:12 Part 009-1000-1124 has a receive time of 1 days and will be available
February 10 2012. It will not meet its required date of January 12 2012.

```

```

17:24:12 Done Scheduling job:MRP00000030135 sending job to queue SaveLoad
17:24:12 Scheduling new unfirm job:MRP00000030244
17:24:48 Part 009-1000-2000 has a receive time of 1 days and will be available
January 13 2012. It will not meet its required date of January 12 2012.
17:24:48 Done Scheduling job:MRP00000030244 sending job to queue SaveLoad
17:24:48 Scheduling new unfirm job:MRP00000030245
17:25:24 Part 009-1000-2000 has a receive time of 1 days and will be available
January 19 2012. It will not meet its required date of January 17 2012.
17:25:24 Done Scheduling job:MRP00000030245 sending job to queue SaveLoad
17:25:24 Scheduling new unfirm job:MRP00000030247
17:25:51 Done Scheduling job:MRP00000030247 sending job to queue SaveLoad
17:25:51 Scheduling new unfirm job:MRP00000030341
17:26:06 Done Scheduling job:MRP00000030341 sending job to queue SaveLoad

```

The information messages are especially useful for discovering which unfirm jobs have potential problems. You can use this generated information to make adjustments to other jobs to prevent a scheduled MRP job from finishing late.

The last line on the MRP Scheduler log contains the Total Non Scheduling Time, which indicates how much time the scheduler spent idle while the MRP processor ran. This section also contains the Scheduled Jobs, the Deleted Jobs, and the Save Load Jobs. For example:

```

23:12:37 MRP process 101 done. Total Non Scheduling Time = 00:24:46. Scheduled
Jobs: 1009 Deleted Jobs: 0 Save Load Jobs: 581

```

## Abandoned Errors

You locate errors in the MRP log by searching for the Abandoned log entries.

This error indicates MRP was unable to finish processing the specific transaction. The Abandoned error is intended as a generic alert that identifies MRP issues, so it can indicate a variety of problems such as timing out and other errors. For example:

```

00:48:24 Building PartList Level: 1
01:49:27 Process 1 not responding. Abandoned during process 'Processing Part~1
91990'
01:49:28 Process 3 not responding. Abandoned during process 'Processing Part~1
92002.215'
01:49:28 Process 102 not responding. Abandoned during process 'Scheduling~MRP0
0000000314'
01:49:28 Building PartList Level: 2

```

When MRP encounters an error, the process pauses an hour to try and correct the error. If nothing resolves it, MRP continues processing as long as enough processors and schedulers are available. If MRP finds enough processors and schedulers, MRP finishes processing the run.

Once the MRP process is complete, you locate the specific cause for the "Abandoned" errors in the AppServer log. First, open the MRP processor log and record the time when the error occurred. You also need to record the processor identifier (PID). Then open the AppServer log and find the entry recorded an hour before the "Abandoned" error on the AppServer log (find the MRP log time and subtract an hour). If the PID matches the log, you can see the specific cause for the error in the AppServer log.

Some typical errors and their resolutions:

- If the main **MRP Control** or **GFS Control** program abandoned the process, you need to cancel and restart the MRP process.
- If you see a **LockWait** timeout error, you can identify which PID caused the lock. The PID that timed out will have an error message in the AppServer log.

## Balancing Processors and Schedulers

A key way you can leverage the MRP logs is to determine the best settings you should use for the **Number of MRP Processors** and **Number of Schedulers** values. You can test run the MRP process through different processor and scheduler values to determine optimal performance.

Typically you should start with 2 processors and 2 schedulers; through this setting, if one fails, the MRP process can still complete. Run the MRP process using these values and record how long it took to finish the run. You now have a set of baseline values to measure other performance times against. Open each of the four logs you generated and search for the **Total Wait/Scheduling Time** value at the end of the MRP process log and the total **Non Scheduling Time** at the end of the scheduler log. These values indicate how long the processor or scheduler was idle until the other processor or scheduler finished generating results. Typically Total Wait/Scheduling Time and Non Scheduling Time values larger than 20 minutes indicate a processor or scheduler was waiting too long.

Experiment with the values to find a performance balance. If schedulers are waiting, add a processor and remove a scheduler; if processors are waiting, add a scheduler and remove a processor. In this way you find the optimal performance balance for the data that moves through a typical MRP process run at your company.

Be aware that each processor and scheduler takes up one central processing unit, or core. You can only enter as many processors or schedulers as the total cores available on your system. For example, if you have eight cores, you should not enter 5 processors and 5 schedulers. If you enter too many cores in the Number of Schedulers and Number of MRP Processes fields, the MRP process will time out and not generate results. Likewise, you must determine how many other processes may require cores at the same time on the server, so be sure you keep enough cores free so other processes can complete successfully.

If you do not know how many cores are available, check the **Pull Max** value on the AppServer. This value defines the core limit available on your system.

## Planning Workbench Job Log

Use Planning Workbench Job Process to execute changes required for jobs created by the Planning Workbench.

The Planning Workbench Job Process is a background task that updates job records with changes required from actions done in the Planning Workbench. You have the option to keep this a process that continuously runs, a process that continuously runs with a delay, or one that a user manually executes. This process generates a log that contains the changes made by this process that you can review if unexpected errors occur.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **PWJob.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Planning Workbench Job Process from this menu location:

**Menu Path:** Production Management > Job Management > General Operations > Planning Workbench Job Process

## Process MRP Recalculation Needed Log

Use Process MRP Recalc Needed to eliminate the need to run a Full Regeneration during the Material Requirements Planning (MRP) process. The process recalculates the demand to find records that typically are ignored when the MRP process runs in Net Change mode.

### Log Options

Available logging options:

- **Log Filename** - Use this field to enter a unique name for your processing. It generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change this directory path.

### Log Location

You launch the Process MRP Recalculation Needed program from this menu location:

**Menu Path:** Production Management > Material Requirements Planning > General Operations > MRP Recalc Needed

## Production Yield Recalculation Log

Use the Production Yield Recalculation Process program to run and schedule production yield recalculation for jobs.

The application will automatically recalculate the expected production yield for jobs that have been flagged for production yield recalculation (this is done by selecting the Production Yield check box on the Job Entry - Header program for the job) on the basis of the operations marked as complete (this is done by selecting the Complete check box on the Labor Entry – Labor Details sheet). Parts used in these jobs (or its operations) must come from sites that have also been flagged for production yield recalculation (this is done by selecting the Production Yield Default option on the site master for the site).

Note, however, that the recalculation process will not result in any action except updating quantity fields on the database, unless one or more production yield system actions have been selected on the site master for every site that stocks a part used in the job (or its operations) and on the Operation master for every operation used in the job.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ProdYieldRecalc.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Locations

You launch the PLM Server Process from these menu locations:

**Menu Path:** System Management > Schedule Processes > Production Yield Recalculation Process

**Menu Path:** Production Management > Job Management > General Operations > Production Yield Recalculation Process

## Refresh PartBin QOH From PartTran Log

Use Refresh PartBin QOH From PartTran program when the PartBin running total is out of balance. The process checks the transactions in the PartTran table and updates the PartBin table quantity balances accordingly.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **FixBinsAllUILog.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Refresh PartBin QOH From PartTran program from these menu locations:

#### Menu Path

Navigate to this program from the Main Menu:

- System Management > Rebuild Processes > Mfg / Distribution > Refresh PartBin QOH From PartTran

## RoHS Job Compliance Log

Use the RoHS Job Compliance Process to run the job compliance roll-up process for the engineered jobs.

You can run the RoHS Job Compliance Process for multiple engineered jobs. The process generates a log file with the compliance status of each assembly, material, operation and substance.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **RoHSJob.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the RoHS Job Compliance Process from this menu location:

**Menu Path:** Production Management > Job Management > General Operations > RoHS Job Compliance Process

## RoHS Part Compliance Log

If you have defined restrictions on the use of certain hazardous substances, you can use the RoHS Part Compliance Process to run the job compliance roll-up process for the engineered parts.

The process generates a log file with the compliance status of each assembly, material, operation, and substance.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **RoHSVendPart.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the RoHS Part Compliance Process from this menu location:

**Menu Path:** Production Management > Engineering > General Operations > RoHS Part Compliance Process

## Multi-Company Logs

---

If your organization has a multi-company license, users can create records that affect two or more companies. Use these logs to make sure these multi-company transactions run without errors and complete as expected.

### Enterprise Configurator Log

If you use the SERVICEBUS data transfer method for multi-company processing, run the Enterprise Configurator Server Process to synchronize configuration data between multiple companies in a single database or companies located in external databases.

This process sends and receives Inter-Company POs and part information from one company to another company.

 **Tip** If you are using the DIRECT data transfer method for multi-company processing, you must use the Enterprise Configurator Direct Server Process instead of the Enterprise Configurator Server Process.

The Enterprise Configurator Server Process synchronizes configuration data between a Manufacturing company and Sales companies (the System Monitor can be used to view transactional activity for these processes). When you run the companion Multi-Company Server Process, it sends the configured part to the Sales companies. They both need to be used to properly synchronize purchase order, sales order and configuration input information between the Manufacturing and Sales companies. To establish regular transfer of data, select the Recurring checkbox, and then attach it to the Startup Task Schedule option. From this point forward, as of the next restarting of the application server, the process automatically transfers the multi-company configuration records as needed.

You run this log to review the data transferred through this process.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ConfiguratorSync.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.
- **Logging Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - **Basic** logging level is the minimum logging level and provides counts of the inbound and outbound records processed
  - **Verbose** logging level generates the same logging as Basic and also provides detailed information for each individual record processed, including the record type, IntQuelID and processing time.
  - **Extended** logging level generates the same logging as Basic and Verbose, as well as a copying the XML document to disk. Multi-Company Direct Server Process writes one XML file to disk and Multi-Company Server Process writes two xml files, one outbound from one company and the second inbound from the other company.

Verbose and Extended logging levels can be used temporarily when trying to understand the flow of data or debug an issue, or they can be kept on if the information they provide is considered helpful.

 **Note** To include verbose logging level record type, IntQuelID and processing time information to the server log entries, add a **<add uri="trace://erp/mc" />** line to the AppServer.config file. This information is useful if an issue is encountered that needs further review by Epicor Support and Development.

## Log Location

You launch the Enterprise Configurator Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > Enterprise Configurator Server Process

## Enterprise Configurator Direct Log

If you are using the DIRECT data transfer method for multi-company processing, use the Enterprise Configurator Direct Server Process to synchronize configuration data between multiple companies in a single database, or companies located in external databases.

This window is valuable for sending and receiving Inter-Company POs and part information from one company to another company.



**Important** If you are using the SERVICEBUS data transfer method for multi-company processing, you must use the Enterprise Configurator Server Process in place of the Enterprise Configurator Direct Server Process for these updates.

The Enterprise Configurator Direct Server Process synchronizes configuration data between a Manufacturing company and Sales companies (the System Monitor can be used to view transactional activity for these processes). When you run the companion Multi-Company Direct Server Process, it sends the configured part to the Sales companies. Both processes need to be used to properly synchronize purchase order, sales order and configuration input information between the Manufacturing and Sales companies. To establish regular transfer of data, select the Recurring checkbox, and then attach it to the Startup Task Schedule option. From this point forward, as of the next restarting of the application server, the process automatically transfers the multi-company configuration records as needed.

## Log Options

Available logging options:

- **Log Filename** - The default file name is **ConfiguratorSyncDirect.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.
- **Logging Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - **Basic** logging level is the minimum logging level and provides counts of the inbound and outbound records processed
  - **Verbose** logging level generates the same logging as Basic and also provides detailed information for each individual record processed, including the record type, IntQuelD and processing time.
  - **Extended** logging level generates the same logging as Basic and Verbose, as well as a copying the XML document to disk. Multi-Company Direct Server Process writes one XML file to disk and Multi-Company Server Process writes two xml files, one outbound from one company and the second inbound from the other company.

Verbose and Extended logging levels can be used temporarily when trying to understand the flow of data or debug an issue, or they can be kept on if the information they provide is considered helpful.



**Note** To include verbose logging level record type, IntQuelD and processing time information to the server log entries, add a **<add uri="trace://erp/mc" />** line to the AppServer.config file. This information is useful if an issue is encountered that needs further review by Epicor Support and Development.

## Log Location

You launch the Enterprise Configurator Direct Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > Enterprise Configurator Direct Process

## Multi-Company Log

Use the **Multi-Company Server Process** to update records across companies on separate databases. These databases can then exchange data through the Microsoft Service Bus application.

You run this process to send and receive inter-company purchase orders, and transfer part, supplier, and customer information from one company to another company. To transfer this data between databases, this process uses Microsoft Service Bus to write multi-company records to the outbound table in the sending company and then this data next updates the inbound table on the receiving company.

You can review the transactions this process generates through a log.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **MultiCompany.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.
- **Logging Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - **Basic** logging level is the minimum logging level and provides counts of the inbound and outbound records processed
  - **Verbose** logging level generates the same logging as Basic and also provides detailed information for each individual record processed, including the record type, IntQuelID and processing time.
  - **Extended** logging level generates the same logging as Basic and Verbose, as well as a copying the XML document to disk. Multi-Company Direct Server Process writes one XML file to disk and Multi-Company Server Process writes two xml files, one outbound from one company and the second inbound from the other company.

Verbose and Extended logging levels can be used temporarily when trying to understand the flow of data or debug an issue, or they can be kept on if the information they provide is considered helpful.



**Note** To include verbose logging level record type, IntQuelID and processing time information to the server log entries, add a `<add uri="trace://erp/mc" />` line to the AppServer.config file. This information is useful if an issue is encountered that needs further review by Epicor Support and Development.

### Log Location

You launch the Multi-Company Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > Multi-Company Server Process

## Multi-Company Direct Log

Use the **Multi-Company Direct Server Process** to transfer global and inter-company data between two or more companies that share the same database. When this process executes, data is transferred between companies set up to share information.

The Multi-Company Direct Server Process sends and receives inter-company purchase orders, inter-company shipments, inter-company invoices, global parts, global suppliers, global customers, global currency information, multi-company GL journal entries, consolidated purchase orders, and all other multi-company related information, from one company to another company. The process is similar to the Multi-Company Server Process, with the only exception that it holds the XML message being transferred between companies in memory rather than transferring the message by Microsoft Service Bus.

## Log Options

Available logging options:

- **Log Filename** - The default file name is **MultiCompanyDirect.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.
- **Logging Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - **Basic** logging level is the minimum logging level and provides counts of the inbound and outbound records processed
  - **Verbose** logging level generates the same logging as Basic and also provides detailed information for each individual record processed, including the record type, IntQuID and processing time.
  - **Extended** logging level generates the same logging as Basic and Verbose, as well as a copying the XML document to disk. Multi-Company Direct Server Process writes one XML file to disk and Multi-Company Server Process writes two xml files, one outbound from one company and the second inbound from the other company.

Verbose and Extended logging levels can be used temporarily when trying to understand the flow of data or debug an issue, or they can be kept on if the information they provide is considered helpful.



**Note** To include verbose logging level record type, IntQuID and processing time information to the server log entries, add a `<add uri="trace://erp/mc" />` line to the AppServer.config file. This information is useful if an issue is encountered that needs further review by Epicor Support and Development.

## Log Location

You launch the Multi-Company Direct Server Process from this menu location:

**Menu Path:** System Management > Schedule Processes > Multi-Company Direct Server Process

## Multi-Tenant Logs

---

If you use a hosted environment such as Epicor Express or SaaS Standard, you can run a number of processes to rebuild and refresh records. Use the logs described in this section to verify these records rebuild accurately.

### ECC Convert Web Customer / Part UOM Log

Use ECC Convert Web Customer / Part UOM to rebuild web customers and part UOMs for ECC for the current company within a Multi-Tenant SaaS environment. You have the options to run the rebuild program for the customer conversion, the Part UOM conversion, or both.

This rebuild process affects only the current company.

## Log Options

Available logging options:

- **Log Filename** - The default file name is **ECCUOMAndCustomerForE10.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Unlock Batch program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Mfg / Distribution > ECC Convert Web Customer / Part UOM

## Fix Book Detail Records Log

Use Fix Book Detail Records to run the rebuild process to fix the Book Detail records for a Sales Order for the current company within a multi-tenant SaaS environment.

This process will update the Book Details records associated with the line of a sales orders.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **FixBookDtl.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Locations

You launch the Fix Book Detail Records program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Mfg / Distribution > Fix Book Detail records

## Fix Book Release Records Log

Use Fix Book Release Records to run the rebuild process to fix and update the Book records for the release of a sales order for the current company within a multi-tenant SaaS environment.

This rebuild process will only affect the current company.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **FixBookRel.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Locations

You launch the Fix Book Release Records program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Mfg / Distribution > Fix Book Release records

## Refresh Order Release Quantity Log

Use Refresh Order Release Quantity to rebuild the order release quantities for sales orders in the current company within for a Multi-Tenant SaaS environment.

This rebuild process will only affect the current company.

## Log Options

Available logging options:

- **Log Filename** - The default file name is **RefreshOrderRelQty.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Unlock Batch program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Mfg / Distribution > Refresh Order Release Quantity

## Remove Orphaned PickedOrders / MtlQueue Log

Use Remove Orphaned PickedOrders / MtlQueue to delete the material queue and picked order records which associated with closed releases are closed for the current company within a Multi-Tenant SaaS environment.

This runs the conversion program CVAM0001, Remove Orphaned PickedOrder and MtlQueue Records. You can run the rebuild process to delete the material queue and picked orders that relate to order releases that are closed and subsequently orphans Picked Order and Material Queue records in a Multi-Tenant SaaS environments. You can verify when the rebuild process completes in the System Monitor. This rebuild process only affects the current company.

## Log Options

Available logging options:

- **Log Filename** - The default file name is **RemoveOrphanedPicksMtlQueue.txt**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

## Log Location

You launch the Remove Orphaned PickedOrders / MtlQueue program from this menu location:

**Menu Path:** System Management > Rebuild Processes > Mfg / Distribution > Remove Orphaned PickedOrders / MtlQueue

## Program Logs

---

Each program contains functionality for adding memos and attaching files. Depending on the record, you can activate and update various logs for tracking changes to records as well.

This section of the guide documents these unique logs. Make sure your users enter data through these powerful logging tools, and they will help your organization track changes and decisions made on specific records.

## Memos

Use memos to enter internal notes or other text related to parts, quotes, customers, suppliers, and employees.

The Memo Maintenance program has a lot of flexibility. You can define the kinds of notes you want to keep and enter them for easy online review by other users.

You can enter both **Comments** and **Memos** within several maintenance programs. Comments are used by other programs and can be printed on reports or forms. Memos, however, are always internal notes and can never be

printed. Each memo can be further identified using Memo Categories. For example, employee memos can belong to categories such as Quarterly Review and Insurance Notes. You can also display memos in trackers.



**Tip** If a record contains one or more memos, a star displays on the **Memo** button on the **Standard** toolbar.

## Fields

### Memo Entry

Fields for the current sheet are listed on this topic.

Some fields on the interface have a context menu, which is indicated by a triangle in the upper right corner of the field. To open the context menu, right-click on the field.

### Memo Description

Displays a description of the memo. This displays when you browse for memo entries.

### Memo Category

Specifies the memo category assigned to this memo. Categories are user-defined in **Memo Category Entry**, and provide additional identification for each memo. This field is optional.

### Memo Text

Contains the text for the memo. Enter free form text that describes the processing situation.

## Add a Memo

1. On the **Standard** toolbar, click **New**.
2. Enter information in the fields that open for data entry.  
Review the **Fields** topic for information on each field.
3. When complete, click **Save** on the **Standard** toolbar.

The record is added to your database.

## Edit a Memo

1. Enter the identifier of the record you wish to edit in the **ID** field or click the **Search** button to find and select the desired record.
2. Edit the record.  
Review the **Fields** topic for information on each field.
3. When complete, click **Save** on the **Standard** toolbar.

The record is updated within your database.

## Delete a Memo



**Important** You cannot delete a record if it is used on another record. For example, if a customer record is on an AR invoice, you cannot delete the customer record.

1. In the **ID** field, enter the identifier of the required record or click the **Search** button to search for and select the desired record.
2. On the **Standard** toolbar, click **Delete**.  
The record is removed from your database.

## Attachments

Use the Attachments function to associate documents and files created by other applications with your parts, quotes, jobs, orders, and so on. One common use of this function is to attach part drawings to a specific part record.

### Attach a File from the Menu Option

1. Launch the program that contains the record for which you want to attach the file. For example, open a sales order in Sales Order Entry.
2. You can attach a file in two ways:
  - a. Click the **Attachment** button on the **Standard** toolbar.
  - b. Right-click on the record in the tree view; from the context menu, select **Add new Attachment...** option.

The **Attachment Management** window displays.

3. Use the fields on this window to find and select the file you want to attach to the current record.



**Tip** For more information on this window, review the **Attachment Management** topics.

4. Click **OK** to close this window.  
The file is now attached to the record. To verify that the file is linked to the current record, a star now displays on the **Attachments** button.
5. Repeat these steps to attach the files you need.

### Attach a File Using Drag and Drop

If at least one file has previously been attached using the attachment menu option (see Attach a File from Menu Option) you can drag and drop files (including emails) to records.

To attach a file using drag and drop:

1. Launch the program that contains the record for which you want to attach the file. For example, open a sales order in Sales Order Entry.
2. If at least one file has previously been attached using the attachment menu option, the Attachments node is available in the tree view of the record. Using your mouse drag a file from Windows Explorer or some other location, or an email from Microsoft Outlook and drop it on the topmost node of the record tree view.
3. The attachment management window opens. Enter a title (or leave title blank to use file name for title) and click **OK**.  
Users who now bring up the record can access the file by expanding the Attachments node.

## Display Attached File

Do the following steps to display a file attached to a record.

1. Find and select a record that has an attachment.
2. You can display the **Attachments** node in these ways:

- a. Click the **Attachments** button (  ) on the **Standard** toolbar.
- b. Click **Actions > Attachments**.
- c. On the tree view, expand the record node and the **Attachments** node.

An **Attachments** sheet now displays within the program. Use this sheet to review the details of each file attached to the current record.

3. To display the attached file:
  - a. From the tree view, double-click the file icon.
  - b. From the Attachments sheet, select the file and click the **View** button.

The attached file displays within its respective program.

## Remove Attached File

You can remove file attachments you no longer need.

Do the following:

1. Open a record that contains an attachment.
2. From the tree view, expand the **<record ID>** node and then the **Attachments** node.  
The files attached to this record display.
3. Select the file you wish to remove.  
The **Attachment** sheet displays.
4. You can remove this attached file in these ways:
  - a. Right-click the attachment you want to delete; from the context menu, select **Remove**.



**Tip** You cannot remove attachments when you display a record in a tracker. When you right-click the attached file, the Remove option is not available.

- b. From the Attachments sheet, select the file. Click the **Delete** button.

The attachment is no longer linked to the current record.

5. Click **Save**.

## Audit Logs

Use the Audit Log to enter comments related to changes made to quote or job records.

If the **Create Audit Log** check box is selected in within **Company Configuration** on the Jobs sheet and you change information on the Job Header sheet for a job marked as **Engineered**, you are prompted to log a description of the changes.

If the **Create Audit Log** check box is selected within **Company Configuration** on the Quote sheet and you change information on the Quote Header sheet for a quote that has been marked as **Quoted**, you are prompted to enter a description of the changes.

You can also use the audit log to review any comments made by other users who made changes to job or quote records.



**Important** For the **Audit Log** command to be active, you must first select a job.

### View the Audit Log

1. Make a change to a job defined as **Engineered** or to a quote defined as **Quoted**.
2. Click **Save** to save the job or quote changes. The **Audit Log** window displays.
3. Enter the appropriate comments to describe why the change was made to the record.
4. Click **Save**.
5. To review previous Audit Log entries, click the **Audit Log** button on the **Standard** toolbar from the program, or click on the **Actions** menu and select **Audit Log**.



**Tip** If an audit log exists for the current record, a star displays on the Audit Log button on the Standard toolbar.

6. Click a record in the **Audit Log** grid on the List sheet or in the Tree View, and then advance to the **Detail** sheet to review the details of that change.
7. When you are done reviewing it and wish to return to the original program, click the **X** in the upper right corner of the window to close the log.

## Call Logs

Use the Call Log functionality to record communications between you and a customer/prospect and to review any conversations that were previously entered in the log. The Call Log is accessible from Customer Maintenance and Opportunity/Quote Entry.

This program contains the following sheets:

- A main **List** sheet that displays all call log entries.
- A **Detail** sheet where you record a new call log entry.
- A **Call Log History Detail** sheet where you can review the details of historical call log entries. Use this sheet to review the details of historical call log entries while you create new entry for the call log.
- A **Call Log History List** sheet that displays all historical call log entries.

## Call Log Overview Fields

Fields for the current sheet are listed on this topic.

Some fields on the interface have a context menu, which is indicated by a triangle in the upper right corner of the field. To open the context menu, right-click on the field.

### Description

Displays a brief description of the call.

### Text

Displays the details about the call/communication.



**Important** The maximum size for call text is **16K bytes** in a **SQL** database. Any text larger than these limits must be broken into more than one call or treated as a document.

### Call Type

Indicates the call type that applies to this call. Select the call type you need from the drop-down list. You create these options within **Call Type Maintenance**.

### Owner

Displays the name of the salesperson who made the call.

## Make a New Call Log Entry

To make a new call log entry:

1. Click the **Call Log** button (  ) on the **Standard** toolbar for the program, click on the **Actions** menu and select **Call Log**.
  2. Click **New** on the **Standard** toolbar to advance to the **Detail** sheet and make your call log entry.
  3. Complete the fields for the entry as outlined in the Field-Level Details section of this help topic.
  4. If you would like to attach a file to this call, click the **Attachments** button (  ) on the Standard toolbar for this program, or click the **Actions** menu and select **Attachments**.
  5. Click **Save** on the **Standard** toolbar, and then close the Call Log to return to the original program.
- 
- Tip** If a call is created for the current record, a star displays on the Call Log button on the Standard toolbar. Likewise, if a file is attached to a call, a star displays on the Attachments button within the Call Log window.
6. Click the **Call Log** button (  ) on the Standard toolbar for this program, or click the **Actions** menu and select **Call Log**.

**7.**

Click the **Search** button (  ) on the **Navigation** toolbar to access **Call Log Search** and browse for call records.

**8.** From the search results, select the record from the **Call Logs** grid that you wish to review.

**9.** Click the tab of the **Detail** sheet.

The selected call log entry displays on the Detail sheet.

**10.** When you finish reviewing entries and wish to return to the original program, close the Call Log window.



**Important** You cannot delete Call Log entries.

## Change Logs

Use the Change Log functionality to view changes made to certain records in the database.

Use this window when you want a complete list of changes made to certain parts of sales orders, purchase orders, quotes, jobs, customers, suppliers, parts, and labor.



**Important** The Change Log is available for programs that use a table which has an assigned ChgLogID. This capability displays on the program's Standard Toolbar as the Change Log icon. If you see this icon, you can enable the Change Log functionality for a given program.

### Enable Change Log for a Program

To activate a change log for a program, select a table and create a new data directive that will write record changes to the applicable program change log.

**1.** Navigate to the **Data Directives** program.

**Menu Path:** System Management > Business Process Management > Data Directives Maintenance



**Important** This program is not available in Epicor Web Access.

**2.** On the **Detail** sheet, do one of the following to select the table for the data directive:

- In **Table**, enter a table name and press **Tab**.
- Click **Table**, use the **Table Search** program to locate the table, and click **OK**.

**3.** In the tree view, select the table and choose **New > New In-transaction Directive** on the **File** menu.

**4.** On the **In-Transaction** sheet:

- a. You must enter a **Directive Name** and select **Enabled**. Other fields are described in the online help for the In-Transaction sheet.
- b. Click **Design** to open the **BPM Workflow Designer**.

**5.** In the BPM Workflow Designer, select the **Change Log** icon and drag it to the workflow design area to begin creating the Change Log action.



**Note** The Change Log item is only available for programs that use a table which has an assigned ChgLogID.

6. In the workflow design area, select the **Start** action and drag one of its connections to a connection on the **Change Log** action.
7. Select the **Change Log** action. In the **Action** statement at the bottom of the workflow design area, click **specified table** to open the **Select Table Field(s)** dialog box.
8. In the list of table fields, use the check boxes to select the fields you want to monitor for change. You can filter the list by typing in **Fields** above the list.  
The **Name** field is inactive, the **Table** field displays the data directive table name, and the filter options for **Added Records** and **Updated Records** are pre-selected and cannot be changed.
9. Click **OK** to close the Select Table Field(s) dialog box.
10. Click **Save and Exit** to close the BPM Workflow Designer and return to the In-Transaction sheet.
11. On the In-Transaction sheet, verify that **Enabled** is selected and choose **Save** on the **File** menu.

Your change log data directive is enabled and running. Changes to records in the data directive table that affect the fields selected in the Change Log action will be written to the change log of the applicable program. To view the change log, click the **Change Log** icon on the program's toolbar.

### Review a Change Log

To review a change log:

1. Click the **Change Log** button on the **Standard** toolbar for this program, or click the **Actions** menu and select **Change Log**.
2. **Tip** If a change log is being generated for a current file, a star displays on the Change Log button.
3. To restrict the changes which display on the log, click on the **List** sheet and enter a **Start At Date**. The log only displays changes made to the record from that date forward. Enter the date directly, or click the down arrow to the right of the field to access a calendar.
4. To sort the grid using the contents of a specific column, click on the tile of the column (**Column Header**). You can sort the log in either descending or ascending order by clicking on a specific column header multiple times.
5. Either click a record on the List sheet or click on a record node in the **Tree View**, and then advance to the **Detail** sheet. You can then review the details of that change.
6. To close the log when you are done reviewing it, click the **X** in the upper right corner of the window. You return to the original program.

## Transaction Logs

Use this program to review information for different types of inventory transactions.

The type of transactions that display depends on the program from which you call this log. For example, if you call the log from the Quantity Adjustments program in the Inventory Management module, the log displays only quantity adjustments to inventory (Type ADJ-QTY).

### Review the Transaction Log

The Transaction Log can only be launched from inventory transaction programs.

1. Click on the **Actions** menu and select **Transaction Log**.
2. Enter the date range for which you would like to review transactions, and then click **OK**.
3. Right-click at the top of the grid to access a context menu that provides options to summarize or group the records in the grid. Other options are also available. For more information, review the **Program Interface - Grids** topic.
4. When you are done reviewing it and wish to return to the transaction program, click the **X** in the upper right corner of the window.

## Purchasing Logs

---

To facilitate purchases, the Epicor ERP application can create purchasing suggestions based on the material needs on open jobs, generate a schedule for purchases, and calculate other purchasing activities. Use the logs described in this section to review these purchasing processes.

### Generate Purchasing Suggestions Log

Use the Generate Purchasing Suggestions process to automatically create a list of suggested purchases based on time-phased information. You create actual purchase orders from these suggestions in Purchase Order Entry.

You must run this process before using New PO Suggestions and Change PO Suggestions. Only one user can run this function at a time.

When generate suggestions, Generate Purchasing Suggestions first references the part or site record for the part's purchase lead time. If there is no purchase lead time on the part or site record, then the Epicor ERP application references the purchase lead time set at the supplier price break level for the part and its primary supplier. The Generate Purchasing Suggestions process builds suggestions from time-phased information, requisitions marked as Send To Purchasing, Unlike Buy To Order (BTO) sales order releases, and purchase contract schedules.

#### Log Options

Available logging options:

- **Log** - Defines the file name used for recording the Generate Suggestions information. Use this field to enter a unique name for your processing logs. These log files can be found on the company's application server in **\\\ServerName\EpicorData\Companies\IRF\Log\[Username]** folder. You use the logs to evaluate the performance of the process, troubleshoot errors, and review the progress of a specific Generate Suggestions processing run.

- **Logging Level** - Use this drop down list to define the amount of information this log records. Available levels:
  - The **Basic** logging level only displays the header information generated for each suggested purchase order.
  - The **Suggestions** logging level displays both the header and detail line information for each suggested purchase order.
- **Number of Processes** - The Number of Processes field defines how many separate threads your server runs to complete the Generate Purchasing Suggestions process. This feature improves performance, as you can split one large Generate Purchasing Suggestions process into several threads. The process then takes less time to complete. Use this value to maximize the performance of the Generate Purchasing Suggestions process.

### Process Performance

The more processors your system can handle, the better system performance you achieve. However if you run the Generate Purchasing Suggestions process against too many processors, you can also slow down performance or even time out the process.

You should run tests to determine what is the ideal number of threads you can run at the same time. To review these performance times, use the Generate Purchasing Suggestions log. You can set this log to run at the Basic level to see the overall time it takes to run the process. If you want more details in the log, select the Suggestions level to see how long it takes to run each process thread by Load Level and part.

Keep in mind that more threads are not always better. As you run your tests, start with a small value to get a base time. Then increase the Number of Processes value for each test. Be sure you always make these changes in small increments. Your performance should improve each run, but you will get to a point where it starts to run slower again. This indicates that your server cannot handle any more process threads, and you need to reduce these threads back to the point where you achieved optimal performance.

### Log Location

You launch the Generate Purchasing Suggestions Process from these menu locations:

**Menu Path:** Material Management > Purchase Contracts Management > General Operations > Generate Suggestions

**Menu Path:** Material Management > Purchase Management > General Operations > Generate Suggestions

## Generate Purchase Schedules Log

Use Generate Purchase Schedules to produce purchase schedules. You can then review and manually adjust the resulting purchase schedules in Purchase Schedule Approval before formal approval.

Before you run Generate Purchase Schedules, use the Generate Purchasing Suggestions process to produce suggestions for scheduled parts. The Generate Purchase Schedules process uses this data to generate the applicable purchase schedules. When running Generate Purchase Schedules, use the Selection sheet to select the parameters for the process, and the Filter sheet(s) to select the specific records to include for the process.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **GeneratePurchaseSchedules.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Generate Purchase Schedules Process from this menu location:

**Menu Path:** Material Management > Purchase Contracts Management > General Operations > Generate Purchase Schedules

## RoHS Supplier Pricelist Compliance Log

Use the RoHS Supplier Pricelist Compliance Process to run the part compliance roll-up for valid and invalid supplier parts in reference to substance restriction rules.

This process generates a log file with the compliance status of each supplier part and substance. This log indicates whether each supplier part is valid or invalid for specific restriction types.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **RoHSVendPart.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the RoHS Supplier Pricelist Compliance Process from this menu location:

**Menu Path:** Material Management > Purchase Management > General Operations > Supplier Pricelist Compliance Process

## Sales Logs

---

Similar to generating purchasing suggestions, the Epicor ERP application has a series of processes that calculate the current demand for your organization's products. It also contains processes that update the options available to customers on configurable parts.

To evaluate how these processes are updating these sales records, use the logs described in this section.

## Demand Entry Logs

When your organization uses EDI, demand records automatically generate, and you can use Demand Entry to review these sales demand records. However if your organization does not use EDI, you can instead use Demand Entry to manually create and process sales demand entries.

This program contains tools to accept, revise, or reject demand entries, lines, and schedules. To evaluate the impact on sales orders, run the logs in Demand Entry to review these automatic or manual demand entries. A separate log is available for the header, line, and schedule levels of each demand record. Based on the log results that display, you can then manually override System Rejected demand entries which have not passed validations based on user-defined rules specified for each customer trading partner. These rules are defined on their customer record.

When you are satisfied with a demand schedule, use the Process action to manually generate the demand. Depending on the demand type, the Demand Entry process creates unfirm order releases, firm order releases, or MRP forecasts. You can then use either Sales Order Entry or Forecast Entry to further refine the resulting data.

**Menu Path:** Sales Management > Demand Management > General Operations > Demand Entry

## Demand Header Log

Use the **Log** selection on the Demand Header submenu to view a comprehensive listing of error messages related to Stop and Warning conditions for the specified demand contract and purchase order number. These explain why the Epicor ERP application rejected and did not process demand. The errors are generated by the Service Connect Workflows when they attempt to process demand received on inbound EDI transaction from your customer trading partner, or when you manually process demand records using Demand Entry or Demand Mass Review.

For example, error messages display for conditions in which the demand entry has failed lead time and other data validations that have been performed when you manually process demand (using the Process selection on the Actions menu) or that have been performed by the Service Connect workflows on inbound EDI transactions. Use the **All Log Entries** check box to specify if all error log entries related to the demand entry should be displayed, or only those for the current demand schedule. For error log entry, it displays the log date, time, detail sequence, schedule sequence, schedule number, error code, action (Stop or Warning), and error log text.

 **Note** Refer to the help for the Customer Maintenance > Customer > Demand and Ship To > Demand sheets, and the **EDI / Demand Management Technical Reference Guide** for detailed information about the error messages that appear on this log, and how to resolve them.

You display this log by selecting an Actions menu option in Demand Entry. To access this log, click **Actions > Demand Header > Log**.

### Detail Fields

#### Detail Fields

Fields for the current sheet are listed on this topic.

Some fields on the interface have a context menu, which is indicated by a triangle in the upper right corner of the field. To open the context menu, right-click on the field.

#### *All Log Entries*

Indicates if all error log entries related to the demand entry should display, or only those for the current demand schedule. Select the check box if all error log entries related to the demand entry should display. Clear the check box if only those error logs for the current demand schedule should display.

#### *Contract*

Displays the identifier number for the demand contract associated with the demand entry error log entries.

#### *Current Sch Number*

Displays the identifier number for the last demand schedule received for the demand entry record that was processed and appears in the demand log.

#### *Demand Log List*

Displays error log messages related to the selected demand contract and customer purchase order number. The entries that appear are dependent on the setting of the **All Log Entries** check box.

For detailed information about the warning and error messages that appear on this log, and how to resolve them, refer to the EDI / Demand Management Technical Reference Guide.

#### *PO*

Displays the identifier number for the customer purchase order associated with the demand entry error log entries.

## List Fields

### List Fields

Fields for the current sheet are listed on this topic.

Some fields on the interface have a context menu, which is indicated by a triangle in the upper right corner of the field. To open the context menu, right-click on the field.

### Action

Displays the action that takes place in the Epicor application (stop transaction or process transaction and display a warning message) when incoming EDI transactions are received with insufficient lead times with respect to the parameters you have specified for that type of transaction.

- If set to **Stop**, the Epicor application marks the demand line as **System Rejected** in Demand Entry; however, you can manually accept the incoming demand by selecting the **Override System Reject** check box. This allows you to designate that the demand schedule/line/demand header can be processed to generate an order or forecast in the Epicor application.
- If set to **Warning**, it designates that the Epicor application has accepted and processed the transaction. Warning messages display on the Demand Log or on the Demand Review Report.

### Demand Contract

Displays identification number for the demand contract for which the Demand Processing error was logged. The field is for display only.

### Detail Sequence

Displays the identifier for the detail line sequence from the DemandDetail or DemandSchedule record to which this DemandLog error is related. If this value is zero, the record is related to the DemandHead record.

### Log Code

When the Service Connect Workflows have attempted to process demand that results from inbound EDI transactions received from your customer trading partner, they automatically generate Demand Log entries both before and after you invoke the Task Monitor to make corrections to invalid data contained in inbound EDI transactions. The following table contains a listing of these generated error codes, and a description of each one:

Error Code	Description
<b>Abort</b>	Log entry generated when a user aborts processing of an inbound EDI transaction file using the Service Connect Task Monitor.
<b>BlankDates</b>	Log entry generated when blank Need By and Ship By dates are identified in the Main_DemandScheduleUpdate workflow.
<b>CTPDates</b>	Log entry generated when an attempt is made to update CTP Ship By or Need By dates.
<b>DemandDetUpdate</b>	Log entry generated for errors identified when updating the DemandDetail table in the Epicor application cannot

Error Code	Description
<b>DemandHedUpdate</b>	be updated by the Main_DemandDetailUpdate workflow.
<b>DemandSchUpdate</b>	Log entry generated when the DemandHead table in the Epicor application cannot be updated by the Main_DemandHeadUpdate workflow.
<b>InvalidContract</b>	Log entry generated for errors identified when updating the DemandSchedule table in the Epicor application cannot be updated by the Main_DemandScheduleUpdate workflow.
<b>InvalidDocument</b>	Log entry generated when an invalid contract is identified in the Main_DemandHeadUpdate workflow.
<b>InvalidPart</b>	Log entry generated when an invalid document is identified in the Main_DemandHeadUpdate workflow.
<b>InvalidRevision</b>	Log entry generated when an invalid part is identified in an inbound EDI transaction file by the Main_DetailPartValidation workflow.
<b>InvalidShipTo</b>	Log entry generated when an invalid part revision is identified in an inbound EDI transaction file.
<b>LeadTimeAdd</b>	Log entry generated when an invalid ship to customer code is identified in the Main_DemandScheduleUpdate workflow.
<b>LeadTimeCancel</b>	Log entry generated when a request is received on an inbound EDI transaction to add a demand schedule and it falls within the <b>Add</b> lead time window.
<b>LeadTimeChange</b>	Log entry generated when a request is received on an inbound EDI transaction to change a demand schedule and it falls within the <b>Change</b> lead time window.
<b>LeadTimeDateChange</b>	Log entry generated when a request is received on an inbound EDI transaction to cancel a demand schedule and it falls within the <b>Cancel</b> lead time window.
<b>LeadTimeNewLine</b>	Log entry generated when a request is received on an inbound EDI transaction to change a demand schedule delivery date and it falls within the <b>Date Change</b> lead time window.

Error Code	Description
<b>LeadTimeQtyChange</b>	Log entry generated when a request is received on an inbound EDI transaction to change a demand schedule quantity and it falls within the <b>Quantity Change</b> lead time window.
<b>LockedDemand</b>	Log entry generated when locked demand is identified in the Main_DemandHeadUpdate workflow.
<b>PartialShipments</b>	Log entry generated when an attempt is made to update a sales order release that has been partially shipped.
<b>PriceDiscrepancy</b>	Log entry generated when comparing the price received on an inbound EDI transaction file, when compared to the Internal price.
<b>Resubmit</b>	Log entry generated when a user resubmits an inbound EDI transaction file for reprocessing using the Service Connect Task Monitor.
<b>UnpostedDemandOnFile</b>	Log entry generated when unposted demand is identified in the Main_DemandHeadUpdate workflow.

### *Log Date*

Displays the date on which the Demand Processing error was logged. The field is for display only.

### *Log Text*

Displays error log messages related to the selected demand contract and customer purchase order number. The entries that appear are dependent on the setting of the **All Log Entries** check box.

For detailed information about the warning and error messages that appear on this log, and how to resolve them, refer to the EDI / Demand Management Technical Reference Guide.

### *Sch Seq*

Displays the identifier for the demand schedule sequence from the DemandSchedule record to which this DemandLog error is related.

- If **zero** displays in this field and in the **Detail Sequence** field, the error message is related to the demand header information.
- If **zero** displays in this field but not in the **Detail Sequence** field, the error message is related to the demand detail information.
- If **zero** displays in this field but not in the **Detail Sequence** field, the error message is related to the demand detail information. DemandDetailSeq are zero, this record is related to DemandHead. If this field is zero but DemandDetailSeq is not, this record is related to DemandDetail. Otherwise this record is related to DemandSchedule.

### Schedule Number

Displays the identifier for the demand schedule to which this DemandLog error is related.

### Time

Displays the time at which the Demand Processing error was logged. The field is for display only.

### Demand Line Log

Similar to the log available on the demand header level, you use the **Log** option on the Demand Line submenu to view a comprehensive listing of error messages related to Stop and Warning conditions for the specified demand line.

The errors are generated either by Service Connect Workflows when they attempt to process demand received on inbound EDI transaction from your customer trading partner, or when you manually process demand records using Demand Entry or Demand Mass Review.

You display this log by selecting an Actions menu option in Demand Entry. To access this log, click **Actions > Demand Line > Log**.

### Demand Schedule Log

Also similar to the log available on the demand header, you use the **Log** option on the Demand Schedule submenu to view a comprehensive listing of error messages related to Stop and Warning conditions for the specified demand schedule.

The errors are generated either by Service Connect Workflows when they attempt to process demand received on inbound EDI transaction from your customer trading partner, or when you manually process demand records using Demand Entry or Demand Mass Review.

You display this log by selecting an Actions menu option in Demand Entry. To access this log, click **Actions > Demand Schedule > Log**.

## Import EDI Demand Log

Use the Import EDI Demand Process to import inbound text-based tilde-delimited EDI transaction files (received from your customer trading partners) that have been passed by the TIE KINETIX eVision third-party application.

These are transactional files that have deposited into the import file destination designated for the specified company in the Company Maintenance > Modules > Sales > Demand sheet. File importation occurs based on a processing schedule that you designate in the Import EDI Demand Process. If erroneous data is identified during direct EDI import processing, you can correct it as required using the Demand Workbench.

### Log Options

Available logging options:

- **Log Filename** - The default file name is **ImportEDI.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Import EDI Demand Process from this menu location:

**Menu Path:** Sales Management > Demand Management > General Operations > Import EDI Process

## Regenerate Configurations Log

Use the Regenerate Configurators Process to regenerate configurations that have been created in the Configurator Designer for base part numbers.

You can specify if all configurations should be regenerated, or if only configurations for individual parts selected in the Filter sheet should be regenerated. When you run this program, it selects previously approved configurations (for which the Approved check box has been selected), and performs the following functions:

- Regenerates associated rules programs
- Regenerates the assigned configuration sequence
- Recalculates internal Has Leave Trigger records

### Log Options

Available logging options:

- **Log Filename** - The default file name is **GenerateConfigurators.log**, and this log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change both the directory path and the file name.

### Log Location

You launch the Regenerate Configurations Process from this menu location:

**Menu Path:** Sales Management > Configurator Management > General Operations > Regenerate Configurations

## Verify Existing Configurations Log

Use the Verify Existing Configurations to verify existing PclnValue records against the current version of the configuration for a base part number.

The utility checks the input value against rules for On Leave, Input Format, and also verifies that the input value is valid in the inputs dynamic list or list items. This utility is valuable when you want to check this information for several configured parts at once.

### Log Options

Available logging options:

- **Log Filename** - Enter the name for the log file. This log generates in the **C:\EpicorData\Companies\[CompanyName]\Processes\[UserName]\** path. If you need, you can change the directory path.

### Log Location

You launch the Import EDI Demand Process from this menu location:

**Menu Path:** Sales Management > Configurator Management > General Operations > Verify Existing Configurations

## System Logs

---

The logs you use most often are the system logs. You activate these logs to help users identify database tables for Business Activity Queries (BAQs) and business methods for Business Process Management (BPM) directives.

You also use these logs to determine the causes of specific issues and evaluate the performance of the Epicor ERP application.

This section of the System Administration Guide documents these important logs. Be sure you understand how to activate, configure, and review these logs.

## Client Tracing Log

Use the **Tracing Options Form** to set up a client tracing log that captures all calls the user interface (client) makes to the server. When you activate this log, any business logic calls sent to the server are automatically recorded within this log.

The client log records transactions between an Epicor ERP client installation and the server. A key tool for troubleshooting issues, activate this log to monitor how this client interacts with the system. The tracing log is a tool that has several uses. Web service developers can use this log to see what business logic calls are made when users launch a specific function; for example, the business logic calls made when a user enters a new customer record. Custom programmers can use this log to fine-tune their customized applications. Epicor Technical Support may also ask you to turn on this log to help them track performance or technical issues.

You can activate this log directly on the client using the Tracing Options Form. Your system administrator can also activate the client log within **User Account Security Maintenance**. When the log is activated on your user account, it automatically generates each time you log into the Epicor ERP application through your user account. If you log into multiple computers through the same user account, a new log generates for each client instance.

Either you or your system administrator can also determine what transactions write to this client log. Several **Dataset Options** are available both on the Tracing Options Form and in User Account Security Maintenance. Activate the options you need; the client log will then write these selected dataset transactions to the client log.

You can turn on **Server Tracing** to include the application server traces to the client log. You can select such traces as Trigger Hits, ERP DB Hits, BPM Logging, BAQ Logging, and use the Other Flags field to add specific traces.

To make this log easier to review, you can organize it by entering **Mark Text** on the Tracing Options Form; all the calls that reference this mark text are then grouped together. You then have the option to display this log either as a .txt file or as an .xml file. Note that a pre-built .xml style sheet is included with this feature. It is recommended that if you want to view the log through the Tracing Options Form, you use the .xml file format. It organizes these calls in a readable format.

 **Tip** You can view these files through **NotePad** or a similar text editor, a web browser (if you save the file in the .xml format), the **Performance and Diagnostic Tool** available from the Epicor Administration Console, or **Microsoft® SQL Server Management Studio**.

### Tracing Options Fields

Fields for the current sheet are listed on this topic.

Some fields on the interface have a context menu, which is indicated by a triangle in the upper right corner of the field. To open the context menu, right-click on the field.

#### Enable Trace Logging

Select this check box to activate the tracing log. All calls made by the user interface to the server now automatically record within the tracing log. If this check box is already selected, it means that the tracing log is active.

## Persist Tracing Options

Indicates whether the selected tracing options are only enabled during the current session. Leave this check box clear if you want to trace the current session activity. Select this check box if you want to record the current and the next session activity.

 **Note** When you log off and log back on, Persist Tracing Options is automatically cleared, so for the next session tracing is turned off. Select this check box if you want to keep the selected tracing options enabled.

## Write Full DataSet

Select this check box to record the entire dataset content including the method parameter structure and data (if any) that passes between the client and the server. Each time a method sends data, it now appears in the client log with the method. When this check box is cleared, only the structure is recorded.

## Track Changes Only

Select this check box if you only want changes to the dataset recorded in the trace log. All changes to columns in the dataset are stored in the log.

## Write Call Context Dataset

If you wish to review the performance of BPM methods and customizations, select the Write Call Context Dataset check box. The Call Context Dataset initializes when a user activates a program (UIApp) that either launches a customized form or a BPM directive. As long as the program is active, method calls are sent to the Call Context Dataset.

## Write Response Data

When a method call has a <returnType> other than void, selecting this check box causes the dataset returned from the server to display on the tracing log. Numerous method calls occur where the data is passed down, modified, not written to the database, and then returned to the client. Selecting this check box places these hidden calls on the trace log. This only applies to datasets that get updated or returned from the server call. Examples of these methods include Credit Checking, Part Verification and Pricing, and GetNewXXX (where XXX is the name of a record). You may need to clear this check box if your system has performance issues when tracing is enabled.

 **Tip** You typically select this option when you are developing a Service Connect workflow and need to see when a non-obvious value is set by a method call. The tracing log displays "Before" and "After" images of the dataset.

## Include Server Trace

Select this check box to include information from server processing in the client trace log. This option is useful if you want to diagnose how client activity affects the application server. For example, select this check box to see what server side calls interact with the client.

You can also add server profiles and traces to the client log. Then when you select the Include Server Trace check box, the client log captures these additional options. Use this feature when you want to track server activity from a client machine instead to reduce the impact on performance. To add these profiles and traces to the client log, update the .sysconfig file that launches the client installation. For more information, review the **Performance Tuning Guide** in the application help. The **Custom Trace Logs** section documents how you add these server options.

## Trigger Hits

When a record is sent to the database to be added, updated, or deleted (Write/Update/Delete), the framework creates an event in which SQL Server intercepts the call and performs table specific logic. After this event is processed, the record is sent to the database. Select this check box to record these trigger events in the server log.

## ERP DB Hits

Activate this check box to track how the Epicor ERP application interacts with the database. You can review each database hit as well as how long it took each hit to complete.

## BPM Logging

Select this check box to record Business Process Management (BPM) method calls. Each time user activity activates a BPM directive, the application server log records the business object method that was called and how long this call took to complete. This option is production friendly.

## BAQ Logging

Select this check box to record Business Activity Query (BAQ) database calls. Each time user activity activates a BAQ, the application server log records which query was called and how long it took this BAQ to gather the data results. This option is production friendly.

## Other Flags (comma delimited list)

Use this field if you want to include additional traces in the log. You can review the available client and server trace options in the Customize Logs chapter of the Performance Tuning Guide. Note that when you enter multiple trace options, you should delimit them using commas.

## Enable EO Browser Trace Logging

Select this check box to record EO Browser error and console messages. ERP programs that have a Kinetic user interface (UI) can be launched as Kinetic applications in the embedded EO Browser. The EO Browser maintains an internal running log that may provide useful information to troubleshoot a problem. The **Enable EO Browser Trace Logging** option allows to silently collect this log and save it to a file on the Epicor application server.

## Log File

Use this field to define the path and file name for the EO Browser trace log. By default, the path is set to **C:\Users\<ClientUserName>\AppData\Roaming\epicor\log** and once the trace is activated, the log is saved to a default txt file - for example, **console7536** (where numbers are random).

You can change the default path either in the Trace Options UI or in the **UserSettings** section of the application server **.sysconfig** file located in the **Client\config** directory. Please refer to the startup configuration documentation in the Application Help for details on EO Browser settings in the app server system configuration file.

## Current Log File

Displays the directory path and filename for the tracing log. If your system administrator activates the client log through **User Account Security Maintenance**, the default directory path defined on the user account displays in this field. However you can enter a different directory path in this field or click the **Browse (...)** button to find and select it. After you click **Apply** or **OK**, this custom directory path becomes the default location that stores the generated log files for this client.

If the client can no longer find this location, the default path specified in the **epicor.exe.config** file is used instead; this .config file is available in the **Client** directory. You enter the directory path and folder you want in the **UITraceFileDefaultDirectory** setting. If the client cannot find this directory path location, the client then writes the client logs to the default **%appdata%\epicor\log** location; for example:  
C:\Users\<ClientUserName>\AppData\Roaming\epicor\log

## Mark Text

Use this optional value to organize the tracing log, making it easier to review. Enter the text you need, then click the **Write** button. All the calls that reference this mark text will group together in the same section of the tracing log. For example:

- abccode lookup



**Tip** Mark Text values also display as options within the .xml version of the tracing log.

## XML File

Defines the directory path and file used for the .xml version of the tracing log. You can enter this path and file name directly or click the **Browse** (...) button to find and select it.

When you have defined the path and filename, click the **Create XML** button. The tracing log now saves using the default .xml format designed for this feature. Any Mark Text values you enter for this log also appear as options on the .xml file.

## Activate From User Account

You or a system administrator can set up the client log to automatically run each time you log in through your user account.

You set up this feature through User Account Security Maintenance.

### 1. Launch **User Account Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

### 2. On the **Detail** sheet, click the **User ID...** button to find and select the user account you wish to update.

### 3. Click on the **Tracing** sheet.

### 4. Select the **Enable Trace Logging** check box.

### 5. Select the **Write Full DataSet** check box to record the entire dataset content including the method parameter structure and data (if any) that passes between the client and the server. Each time a method sends data, it now appears in the client log with the method. When this check box is cleared, only the structure is recorded.

### 6. Select the **Track Changes Only** check box if you only want changes to the dataset recorded within the tracing log. All changes to columns in the dataset are then stored within the log.

### 7. Activate the **Include Server Trace** check box when you want to track the client's interaction with the server. This creates a <serverTrace> node within trace packets (<tracePacket>) in the client tracing log. Use the database activity gathered in this section to review how the client installation may be affecting the performance of the server.

**Tip** You can add server profiles and traces to the client log. When you select the Include Server Trace check box, the client log captures these additional options. To add these profiles and traces to the

client log, update the .sysconfig file that launches the client installation. You can also customize what the tracing log tracks by creating a client configuration file that contains additional tracing options and logging levels. These custom options are used when you activate the client tracing log.

For more information, review the **Performance Tuning Guide** in the application help. The **Custom Trace Logs** section documents how you add these server profile and custom trace options.

8. Use the **Write Call Context Dataset** check box to include Business Process Management (BPM) table values on the trace log. This information provides the data context for a call each time a call is sent between the client and the server. This information is useful for developing BPM method directives, as you can intercept these calls to run additional processing that verifies data and other custom functions.
9. Numerous method calls occur where the data is passed down, modified, not written to the database, and then returned to the client. Select the **Write Response Data** option to include these database transactions on the trace log. This only applies to datasets that get updated or returned from the server call.



**Note** You may need to clear this check box if your system has performance issues when tracing is enabled.

10. Now select the **Log Directory Scheme** option for the default log directory. The option you select defines the directory path scheme for this client account.

Available options:

- %appdata%\epicor\log\
- %temp%\epicor\log\
- %localappdata%\epicor\log\
- **Default from Epicor.exe.config file** -- Select this option to use the path defined in the Epicor.exe.config file; this config file is located in the **Client** directory for each Epicor ERP installation. You enter the directory path and folder you want in the **UITraceFileDefaultDirectory** setting.

Notice after you select a scheme option, the **Current Log Directory** field displays the default directory path and folder that gathers the client logs for this user account.



**Tip** Users can override this default path on each client. When they display the **Tracing Options Form** on the client, they can enter a different path in the **Current Log File** field. The log files then generate in this folder and this custom directory path becomes the default Current Log Directory for this client.

However if the client can no longer find this location, the default path specified in the **epicor.exe.config** file is used instead; this .config file is available in the **Client** directory. If the client cannot find this directory path location, the client then writes the client logs to the default **%appdata%\epicor\log** location; for example:  
C:\Users\<ClientUserName>\AppData\Roaming\epicor\log

11. Click **Save**.

The next time a user launches the Epicor ERP application with this account, the client log automatically generates using your selected Dataset Options. It generates either in the default file location specified on the user account or a unique directory entered by the user on the client through the **Tracing Options Form**.

A new log file is created each time the user logs into the application with this user account. If the user logs into multiple computers through the same user account, a new log generates for each client instance. When you have gathered enough information, access the user account and de-activate the client tracing log.

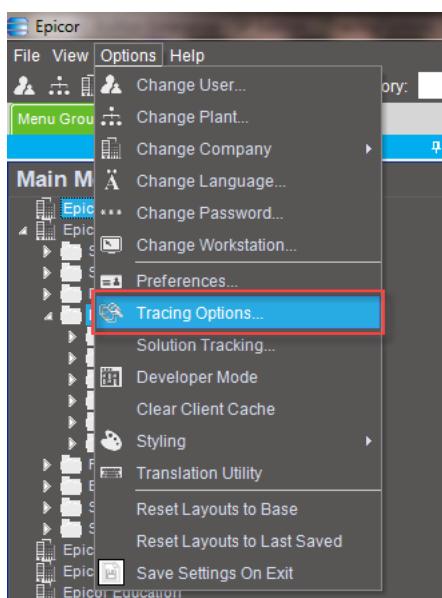
## Activate From Client

Use the **Enable Trace Logging** check box to activate the Tracing Log. You then select what information you want to include in the log.

This topic explains how you can manually activate the tracing log directly from the Epicor ERP client. However a system administrator can also set up your user account so the tracing log automatically launches each time you log into the application. This feature is available within **User Account Security Maintenance**; the system administrator can activate the client log on the **Tracing** sheet.

1. Launch the **Tracing Options Form**. Depending on interface style, you launch this window in different ways:

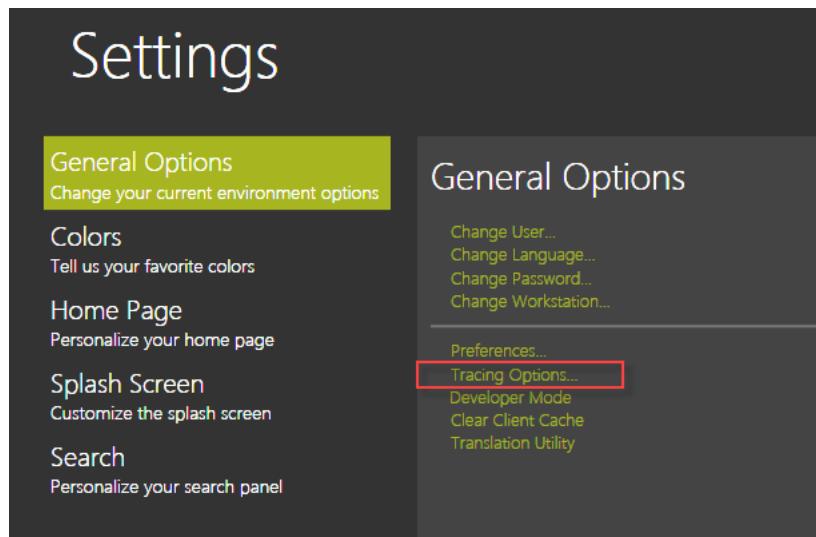
- a. When you run the application using the **Classic Menu**, from the **Main Menu** window you click **Options > Tracing Options**.



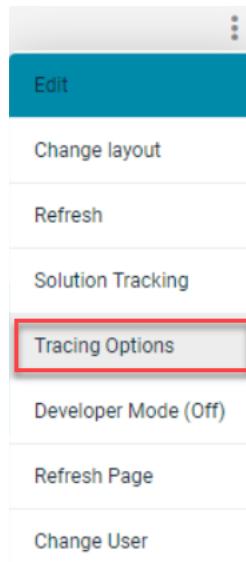
- b. When you run the application using the **Modern Home Page** interface, you can activate the trace log in a couple ways. Click the **Down Arrow** at the bottom of the window to display the toolbar, then click the **Tracing Options** button.



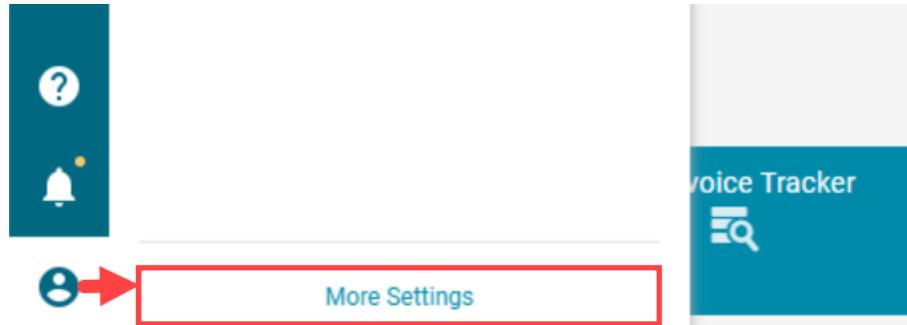
- c. You can also launch this window by clicking the **Settings** tile. From the **General Options**, select **Tracing Options**.



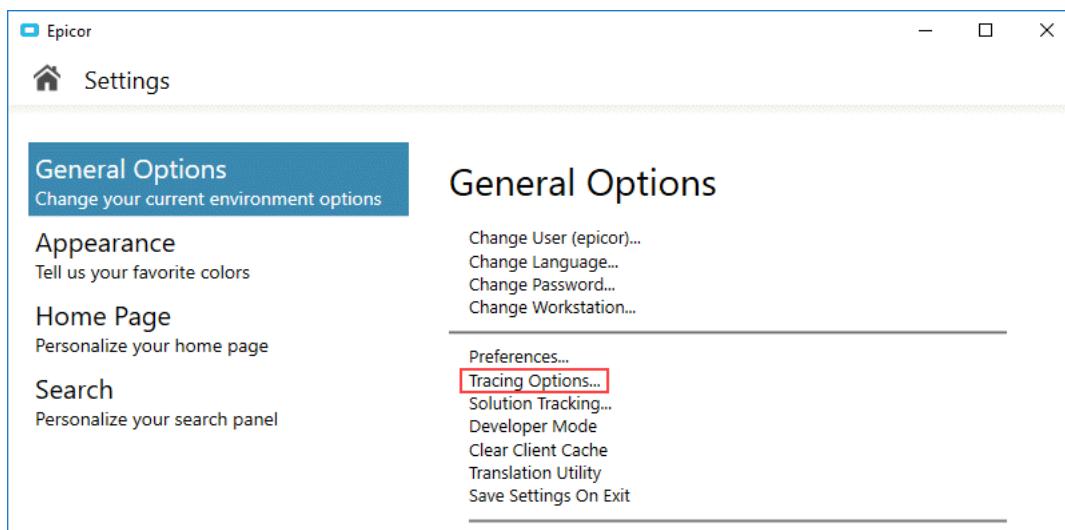
- d. If you run the application using the **Kinetic Home Page** style, on the Home Page, select **Tracing Options** from the overflow menu.



Alternately, click the **User** icon at the bottom left corner of the window and select **More Settings**.



Then on the **Settings** page, select **General Options > Tracing Options**.



The **Tracing Options Form** displays.

2. Now select the **Enable Trace Logging** check box to activate the log.  
Selecting this option activates the tracing log check box options available on this window.
3. Select the **Write Full DataSet** check box to record the entire dataset content including the method parameter structure and data (if any) that passes between the client and the server. Each time a method sends data, it now appears in the client log with the method. When this check box is cleared, only the structure is recorded.
4. Select the **Track Changes Only** check box if you only want changes to the dataset recorded within the tracing log. All changes to columns in the dataset are then stored within the log.
5. Use the **Write Call Context Dataset** check box to include Business Process Management (BPM) table values on the trace log. This information provides the data context for a call each time a call is sent between the client and the server. This information is useful for developing BPM method directives, as you can intercept these calls to run additional processing that verifies data and other custom functions.
6. Numerous method calls occur where the data is passed down, modified, not written to the database, and then returned to the client. Select the **Write Response Data** option to include these database transactions on the trace log. This only applies to datasets that get updated or returned from the server call.



**Note** You may need to clear this check box if your system has performance issues when tracing is enabled.

7. Activate the **Include Server Trace** check box when you want to track the client's interaction with the server. This creates a <serverTrace> node within trace packets (<tracePacket>) in the client tracing log. Use the database activity gathered in this section to review how the client installation may be affecting the performance of the server. When you select the **Include Server Trace** check box, server trace options become enabled:
  - a. If you select the **Trigger Hits** check box, when a record is sent to the database to be added, updated, or deleted (Write/Update/Delete), the framework creates an event in which SQL Server intercepts the call and performs table specific logic. After this event is processed, the record is sent to the database. Select this check box to record these trigger events in the server log.
  - b. Activate the **ERP DB Hits** check box to track how the Epicor ERP application interacts with the database. You can review each database hit as well as how long it took each hit to complete.

- c. Select the **BPM Logging** check box to record Business Process Management (BPM) method calls. Each time user activity activates a BPM directive, the application server log records the business object method that was called and how long this call took to complete. This option is production friendly.
  - d. Select the **BAQ Logging** check box to record Business Activity Query (BAQ) database calls. Each time user activity activates a BAQ, the application server log records which query was called and how long it took this BAQ to gather the data results. This option is production friendly.
  - e. Use the **Other Flags (comma delimited list)** field if you want to include additional traces in the log. You can review the available client and server trace options in the Customize Logs chapter of Performance Tuning Guide. Note that when you enter multiple trace options, you should delimit them using commas.
- 8.** Select the **Enable EO Browser Trace Logging** option to capture EO Browser error and console messages to a log file.  
 ERP programs that have a Kinetic user interface (UI) can be launched as Kinetic applications in the embedded EO Browser. The EO Browser maintains an internal running log that may provide useful information to troubleshoot a problem. The **Enable EO Browser Trace Logging** option allows to silently collect this log and save it to a file on the Epicor application server.
- 9.** Click the **Apply** to confirm your changes.
- 10.** Click **OK** to close the **Tracing Options Form**.  
 Now actions you perform in Epicor ERP are recorded in the tracing log.

## View the Tracing Log

This topic explains how you can examine the information captured by the Tracing Log.

- 1.** Click the **View** button.
- 2.** The tracing log displays in **Notepad**.

Notice each method call made from the client is recorded in the **<TracePacket>** tags.

Displayed information:

Log Entry	Description
<b>&lt;businessObject&gt;</b>	Business objects define the various processes run by the Epicor ERP application. For example, the Part business object handles all the processing done on a part record.
<b>&lt;methodName&gt;</b>	A method is a process that runs from a business object. Any process like adding a record (GetNew) or saving a record (Update) occurs when the method runs.
<b>&lt;returnType&gt;</b>	The items manipulated by the method. Typically Epicor business objects return either datasets (related sets of data) or void when the dataset passed through the input parameter.
<b>&lt;localTime&gt;</b>	The date and time stamp when the method was run.
<b>&lt;executionTime&gt;</b>	Indicates how long it took the method to run in milliseconds. This tag breaks down this time duration into the following categories: <ul style="list-style-type: none"> <li>• <b>total</b> - Displays the length of time it took for the entire method call to run from start and finish. This value includes the retries the call made to the server (if any).</li> <li>• <b>roundTrip</b> - Contains the length of time it took the call to go to and return from the server. This value only displays the length of time for the successful call; it does not include any retries.</li> </ul>

Log Entry	Description
	<ul style="list-style-type: none"> <li><b>channel</b> - Details how long it took channel management to create a new channel and remove stale channels (TTL).</li> <li><b>bpm</b> - Displays how long Business Process Management (BPM) took to run the BpmContext method (if this call was sent).</li> <li><b>bpmDataForm</b> - Displays the time a BPM data form was open for data entry.</li> <li><b>other</b> - Contains any time not accounted for in the above categories. This value is calculated by subtracting the other categories from the total time (other = total - roundTrip - channel - bpm). Reasons for this additional time include how long it takes to run the trace and how long it took to run the conversion between datasets and tablesets (DatasetAdapter).</li> </ul>
<retries>	Indicates the number of times the call was re-sent to the server (if any). When a call fails to reach the server, the application sends it again. This additional call is recorded as a retry.
<parameters>	Input parameters unique for each method. The business object method requires these Types in the specified order to provide expected behavior.
<ServerTrace>	Displays the portion of the server log belonging to the particular client (user) activity.

Within the server log, the following information is recorded:

Type	Description
<b>Utc</b>	The time the call was received in UTC time.
<b>act</b>	The message action (indicates the service and method being called).
<b>dur</b>	The duration of the server call in milliseconds.
<b>cli</b>	The IP address of the calling client. ":1:XXXXX" indicates the call was made from the same machine as the server.
<b>usr</b>	The identifier of the calling user.
<b>tid</b>	The thread ID assigned to handle the call.
<b>pid</b>	The server process ID.

3. Scroll through the log to see all the trace packets you activated.



### Example

```

<tracePacket>
  <businessObject>Ice.Proxy.BO.NamedSearchImpl</businessObject>
  <methodName>GetRows</methodName>
  <appServerUri>net.tcp://1229681/ice3/</appServerUri>
  <returnType>Ice.Tablesets.NamedSearchTableset</returnType>
  <localTime>1/26/2016 16:48:08:4282007 PM</localTime>
  <executionTime total="215" roundTrip="139" channel="68" bpm="0" other="8" />
  <retries>0</retries>
  <parameters>
    <parameter name="whereClauseNamedSearch" type="System.String"><![CDATA[ProductID = 'EP' AND SearchForm = 'Security Group Search' AND CalledFrom = 'Ice.UI.SecGroupEntry.dll' AND UserId = 'MANAGER']]></parameter>
    <parameter name="whereClauseControlSetting" type="System.String"><![CDATA[ControlSetting = '1']]></parameter>
  </parameters>

```

```
[CDATA[ ]]></parameter>
    <parameter name="whereClauseWhereClause" type="System.String"><! [ CD
ATA[ ]]></parameter>
    <parameter name="pageSize" type="System.Int32"><! [ CDATA[ 0 ]]></param
eter>
    <parameter name="absolutePage" type="System.Int32"><! [ CDATA[ 0 ]]></p
arameter>
    <parameter name="morePages" type="System.Boolean"><! [ CDATA[ False ]]>
</parameter>
</parameters>
</tracePacket>
```

## Organize the Tracing Log

You can organize the tracing log so it is easier to review.

1. In the **Mark Text** field, enter a value by which you want to organize the log.
2. Click the **Write** button.

All the calls that reference this mark text will be grouped together in the same section of the tracing log.



### Example

```
<tracegroup name="October11" />

<tracePacket>
    <businessObject>Ice.Proxy.Lib.BOReaderImpl</businessObject>
    <methodName>GetRows</methodName>
    <returnType>System.Data.DataSet</returnType>
    <localTime>11/10/2017 16:54:31:9522427 PM</localTime>
    <executionTime>187</executionTime>
    <parameters>
        <parameter name="serviceNamespace"
type="System.String"><! [ CDATA[ Ice:BO:Company ]]></parameter>
        <parameter name="whereClause" type="System.String"><! [ CDATA[ Company =
'EPIC06' ]]></parameter>
        <parameter name="columnList"
type="System.String"><! [ CDATA[ ESEURL,ESENNotificationSourceID ]]></parameter>
    </parameters>
</tracePacket>
```

## Convert the Log Into .xml

You can save the tracing log in the default .xml format and view within any web browser. The Mark Text values you enter for this log also display as options on the .xml file.

1. To specify the .xml file you can either:
  1. Enter the path manually and specify the name of the .xml file.



### Example

```
C:\ProgramData\Epicor\log\MyClientLog.xml
```

2. Browse to the path where you want to store the .xml file.

2. Click the **Create XML** button.

The .xml is created and the information you specified in **DataSet Options** pane displays in this .xml format.

## Remove All Tracing Log Entries

You may need to delete all entries from the log.



**Example** You want to clean the log from previous entries and start tracking the current activity to search for any potential issues that affect the current poor performance of your client.

1. To remove the information from the log, click the **Clear Log** button.

2. Click the **Apply** or **OK** button to confirm your changes.

The client log no longer contains the transactions it previously recorded. You can now record new transactions to this log.

## Conversion Log

When you upgrade the Epicor application to a new version, you can launch the **Conversion Workbench** to run conversion processes against your data. The upgraded data is then compatible within the new version.

To see the progress of a data conversion, you review the **Conversion Log**. If the conversion resulted in an error, use this log to determine whether the error was caused by the system or a data issue.

### Log Location

You display the Conversion Log from this menu location:

**Menu Path:** System Management > Upgrade/Mass Regeneration > Conversion Workbench



**Important** This program is not available in Epicor Web Access.

After you have run a conversion through the **Conversion Workbench**, either double-click the conversion entry or click **Actions > Maintain Conversion Program** to display **Data Conversion Maintenance**. Through this program, you review details about the selected conversion process. Click the **Conversion Log** tab to review the log results.

## Database Migration Log

During the upgrade process, you most likely will also migrate your database(s) to the current version. This ensures the database(s) are synchronized with the current schema.

When you run the database migration process, a log automatically generates that records the migration results. You can then verify whether the migration ran without errors.

To view this log, access your server machine. Then using Windows Explorer, navigate to this directory path:

- **C:\Program Files (x86)\Common Files\Epicor Software Corporation\Database Manager Extensions\3.0.<x>\DB Migration\<db name>\_Results.txt**

Substitute the name of your database for the <dbname> value.

## Error Message Log

If an issue causes an error message to display, you have several features for viewing the log details.

Error messages display in a dialog box. This dialog box has options for reviewing the logged details for the message. To display, print, email and/or save the error message log:

1. Click the **Detail** button to display the error message log.

The dialog box expands, showing you the following information:

- **Application Error** - Displays the application error generated by the system.
- **Error Detail** - Contains the primary information about the error, including the **Message** that displays, the **Program** which initiated the error, and the **Method** that generated it.
- **Client Stack Trace** - Displays the call trace that generated from your client installation.
- **Inner Exception** - Contains the server stack trace and the exception thrown by the system.

2. Click the **Summary** button to restore the original error message view.

3. Click the **Print** button to make a hard copy of the error message log.

The **Print** window displays.

4. Now print the error message log.

- a. From the **Name** drop-down list, select printer to which you will send the application error log.

- b. Click **OK**.

The error message log is printed on the selected printer.

5. Click the **Email** button to send the error details in an email.

The **EMail Message** window displays.

- a. Type in the recipient's email address in the **To** field.

- b. If you want to send a copy of this email to other recipients, add their email addresses into the **Cc** field.

- c. In the Toolbar, click **Send**.

6. You can also copy and save the error message log to a file. To do this, in the error message dialog, click **Copy**.

The error log is added to the clipboard.



**Note** This action also adds some system information to the error log. This system information includes:

- **AppServer Connection** - specifies the application server address and the ERP instance - for example, **net.tcp://EpicorServer/ERP102700**.
- **Form Name** - specifies the name of the ERP program the error occurred in - for example, **Sales Order Entry**.
- **Customization Name** - specifies the name of the customization layer applied to the current program, if any.
- **Menu ID** - specifies the menu ID of the ERP program - for example, **OMMT3001**.
- **Software Version** - specifies the ERP version - for example, **10.2.700.3**.

7. Open a text editor like **Notepad** or a similar text editor.

8. **Paste** the error message log.

The error message and related system information now display in the text editor.

9. **Save** the error message log.

You now have an error message file you can send to your Epicor consultant or Epicor Technical Support.

## Global Alert Message Error Log

The Global Alert Error Log tracks issues that occur with global alerts.



**Important** The AlertLog table is no longer used to record new alerts. You can only view and delete existing alert errors that occurred whenever the application was unable to send a global alert to a specified recipient.

### Log Options

You can filter the log through the following options:

- **Starting At Sender** - Enter the number of the first global alert you wish to review. All global alert errors that begin or come after this number displays in the search results.
- **Sent Date** - Defines the date on which you want to review the global alert errors.
- **Alert Type** - You can filter the results by type. Available options:
  - **Global Alerts**
  - **Shop Warnings**
  - **Change Log Alerts**
  - **All**

After you define the filter options you need, the Global Alert Error Log window displays entries that match your search parameters.

### Log Location

You launch the Global Alert Message Error Log from this menu location:

**Menu Path:** System Management > Schedule Processes > Global Alert Message Error Log

## Server Log

The server log records the transactions the server makes with client installations and the network. Just like the client log, the server log is a key tool for troubleshooting issues.

You activate this log within the Epicor Administration Console. Launch this program and then expand the Server Management node, your [ServerName] node, and your [AppServerName] node. You can then access the Application Server Settings window.

## Application Server Settings

You use the Application Server Settings window to set up logging settings, for example, when you are experiencing performance issues.

The below two sections are found on this form:

- **Application Settings** - the BAQs fields can improve how business activity queries gather data and run on your system; use these fields to optimize query processing.
- **Tracing Settings** - activate and configure the application server log to help determine the cause of slow performance. You define the level of information to be tracked and specify your **File** output properties. You can then display the file log within the Performance and Diagnostic Tool, send this log to Epicor Technical Support or your Epicor consultant. You can also choose to publish the server log traces to **Application Insights** Azure resource and use analytic tools to diagnose issues or view performance.

 **Tip** You should always generate application server logs before you contact Epicor. The technicians and consultants will ask for this information, so you will reduce how long it takes to resolve your issue by gathering performance data in advance. The System Administration Guide describes what logs you should generate before you contact support. The Performance Tuning Guide details how you can further customize server logs to capture the operations and activity you need to review. Both guides are located in the application help; navigate to the System Management > Working With... node in the Table of Contents pane.

1. From either the **Action** menu or the **Actions** pane, select **Application Server Settings**.

The **Application Server Settings** window displays.

2. The following is the list of **Application Settings**:

- a. For the **BAQ Query Max Result Rows** field, leave the default setting at 0, indicating there is no row limit.

If you have a BAQ that is returning a large number of rows and is affecting performance, enter a value (number of rows) in this field to limit the number of rows returned. This is similar to using the TOP clause in SQL.

 **Tip** If you do limit rows, you may not see a record you are expecting. Instead of entering a value here, consider adding or adjusting criteria to your BAQ to make it more efficient.

- b. Now in the **BAQ Query Timeout** field, enter how many seconds can elapse before the application server stops the query.

By entering a value in this field, you define how long each BAQ is allowed to run. When a query attempts to generate results and reaches this time limit, the application server stops the query and sends the user a time out message. The default value is 0, indicating there is no limit. By entering 900, you allow queries to run 15 minutes before they time out.

- c. Use the **Global Access Scope ID** field to set a default Access Scope for the entire Epicor ERP application server. This optional field contains the list of Access Scopes - both active and inactive that are set up in this ERP application server.

An Access Scope groups one or more ERP services, specific service methods, and/or Business Activity Queries (BAQs) under an Access Scope ID.

 **Important** Note that if you set a Global Access Scope, all users of the Epicor ERP application server, including Security Managers (SMs) and Global Security Managers (GSMs), will only have access to the ERP entities - Business Object services, their methods, and/or BAQs - explicitly specified

in this Access Scope. All services not specified in the Global Access Scope will be denied to all users including SMs and GSMS.

However, if a certain user is assigned to an Access Scope different from the enabled Global Access Scope, at runtime, such user Access Scope will override the server Global Access Scope.

**3.** You then use the rest of the fields on this window to activate the application server log and determine what information this log gathers. First, select the **Trace Log Enabled** check box.

**4.** Specify the **Log File** settings:

- a. Enter the **File Location**. This field indicates where you want the application server log to generate. Either enter this path directly or click the **Browse (...)** button to find and select this directory path. Note the log file name is automatically appended with **date** it was created on.



**Note** By not entering a value in this field, Epicor file logging is disabled. You may, however, set up file logging through the Serilog settings directly in **AppServer.config** file. See the **Advanced File Logging Configuration** topic for more information.

- b. To avoid running into disk space issues, you can control the size and number of logs you want to maintain. Use the **Max Log File Size** field to define how large you will allow each file to grow. Enter the size limit and then select a size option from the accompanying drop down list. Available options:

- **Bytes**
- **Kilobytes**
- **Megabytes**
- **Gigabytes**

- c. When each log file reaches this size limit, it creates a new log file. To limit how many log files the application server will create, enter a number in the **Max Log Files** field. The application server will generate this number of log files and then it will stop gathering server log data.

**5.** To publish the Server log traces to Application Insights service accessible from within the Microsoft® Azure® portal, specify your instrumentationKey in the **Application Insights Key** field.

You obtain this key on the Azure portal page on your Application Insights dashboard.

The screenshot shows the Azure Application Insights dashboard. On the left, there's a list of resources under 'Application Insights'. In the center, there's an 'Overview' section with links for 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. On the right, there's a detailed view of a resource named 'Applicationinsight\_qa'. It shows details like 'Resource group (change) application\_resource', 'Location East US', 'Subscription (change)', and 'Subscription ID'. A red box highlights the 'Instrumentation Key' input field, which contains a long alphanumeric string.

**6.** Next define what **Standard Logging** information you want the application server log to record. If you only are tracking a specific database activity, just activate one of the specific options. Server logs are easier to review if you only capture the types of database activity you require. Be aware that some options do not harm performance (production friendly), while other options can reduce performance. Available options:

- a. **Verbose Logging** - The default option, select this check box when you want the log to record all calls, triggers, and exception messages sent to the application server. If you wish to see any business logic exceptions, you must select this check box. This option is production friendly.

- b. **Trigger Hits** - When a record is sent to the database to be added, updated, or deleted (Write/Update/Delete), the framework creates an event in which SQL Server intercepts the call and performs table specific logic. After this event is processed, the record is sent to the database. Select this check box to record these trigger events in the server log.
- c. **ERP DB Hits** - Activate this check box to track how the Epicor ERP application interacts with the database. You can review each database hit as well as how long it took each hit to complete.
- d. **BPM Logging** - Select this check box to record Business Process Management (BPM) method calls. Each time user activity activates a BPM directive, the application server log records the business object method that was called and how long this call took to complete. This option is production friendly.
- e. **BAQ Logging** - Select this check box to record Business Activity Query (BAQ) database calls. Each time user activity activates a BAQ, the application server log records which query was called and how long it took this BAQ to gather the data results. This option is production friendly.



**Tip** Remember that the **Verbose Logging**, **Detailed Exceptions**, **BPM Logging**, and **BAQ Logging** options are production friendly.

7. Indicate which **Advanced Logging** information you want to include on the application server log. These options record calls from the overall system server, and may impact performance while active. Available options:
  - a. **System DB Hits** - Select this check box to record all the hits the database receives from SQL Server. Use these values to determine the performance of SQL Server.
  - b. **System Table Methods** - Activate this check box to track the method calls being placed against the system tables.
  - c. **SQL Query Detail** - Select this check box to have the application server log include the details of the SQL queries performed by the application.

8. When you finish making your selections, click **Apply** and then **OK**.

9. The **Server Manager** dialog box displays, asking if you want these log settings to activate. If this is a good time to begin generating results in the application server log, click **Yes**.



**Note** Your selected trace log settings are written to the **AppServer.config** file and applied without the need to restart the application server.

When you select a tracing option, you activate the <TraceFlag> setting in this configuration file, and these settings determine what the application server log records. The AppServer.config file is typically located in C:\<YourEpicorInstallation>\<YourEpicorVersion>\Server\ directory.



**Important** After you gather the system information you need, be sure to return to the Epicor Administration Console and de-activate your log setting options. This reduces unnecessary calls to the server and improves performance.

This tracing log records any business logic exceptions internal to the Epicor ERP application. For example, this log records an error when too many characters are entered in a field, a record already exists, how long it takes a business object method to run, and so on.

Any errors that occur outside of the internal business logic are not recorded in the application server log. Examples of items not captured by this log include framework exceptions, security exceptions, fatal errors, and similar items. You can review these errors through the **Event Viewer**. You access this Windows tool through a control

panel. Launch the **Administrative Tools** control panel; the Event Viewer displays as a shortcut. You can send this shortcut to your desktop for easier access.

## System Activity Log

Use the **System Activity Log** dashboard to review the system activities occurred within the application.



**Important** In **Epicor Cloud ERP - Multi Tenant** or **Epicor Cloud ERP - Dedicated Tenancy**, this program or feature may not be available or may operate under certain restrictions.

The **System Activity Log** tracks four activity types:

- **Log on Failures** - Users could review this activity type to check for hacking.
- **User Log On** - Which users logged into the application and when they logged in.
- **User Log Out** - Which users logged out of the application and when they logged out.
- **Company Tracking Status** - Any changes made to the Company record.

You can locate the activity you wish to review by filtering the data activity that displays through the available search fields.

To use this log, you first need to activate it within **Company Maintenance**. As users perform system activities, this log records these entries. You then launch the System Activity Log and review this activity by filtering on a specific user, date range, both user and date range, or other options. Later you remove selected entries from this dashboard by running the **System Activity Log Purge** program.

**Menu Path:** System Setup > Security Maintenance > System Activity Log

### System Activity Log > Fields

Fields for the current sheet are listed on this topic.

Some fields on the interface have a context menu, which is indicated by a triangle in the upper right corner of the field. To open the context menu, right-click on the field.

#### ActivitySeq

Contains the identifier assigned by the system to the database activity.

#### ActivityType

Defines what database action occurred. For example, this column can indicate new business activity queries (BAQs) were created.

#### Company

Indicates the company for which the database change was made.

#### Table Name

Displays the specific table within the database which was affected by the system activity.

#### User ID

Displays the identifier for the user who made the database change.

## Activate the Log

You activate system logging by selecting an option within Company Maintenance. You then stop and restart the application pool.

**1.** Navigate to **Company Maintenance**.

**Menu Path:** System Setup > Company/Site Maintenance > Company Maintenance



**Important** This program is not available in Epicor Web Access.

By default, the **General Settings** sheet displays; locate the **Activity Tracking** group box.

**2.** Select the **System Activities** check box.

**3.** **Save** the company record.

**4.** Repeat these steps for each company you want to track system changes.

The System Activity Log now activates. It records system changes for each company you selected.

## Filter the Data

Follow these steps to filter and run the System Activity Log.

**1.** Launch the **System Activity Log**.

**Menu Path:** System Setup > Security Maintenance > System Activity Log

**2.** Use the **Table Name** field to filter the log to only display database activity that occurred for a specific table.

**3.** Use the **ActivityType** field to limit the log to only display a specific database action, like Created or Deleted, in the results.

**4.** To filter the log to only display database changes made by a specific user, enter the user identifier you need within the **User ID** field.

**5.** To limit the data activity to only display items that occurred within a date range, enter a start date and an end date in the **Date** fields.

**6.** Besides using these filter values individually, you can also use them in combination to filter the results. When you are ready to display the database activity, click the **Refresh** (  ) button.

The **System Activity** grid populates with the database activity that matches your search parameters.



**Tip** This log is stored on the **Ice.sysactivitylog** table.

## Purge Selected Records

Since this log tracks database activity, the amount of information saved by this program can cause a database to quickly grow in size.

When you no longer need to review some system activity logs, use the System Activity Log Purge to find, select, and remove specific log entries.

### 1. Launch **System Activity Log Purge**.

**Menu Path:** System Management > Purge/Cleanup Routines > System Activity Log Purge



**Important** This program may not be available, or operate under certain restrictions in Epicor Cloud ERP.

### 2. Click **Search** to find and select the system activity records you want to review.

### 3. Click the **List** sheet.

The selected system activity records display on the **System Activity List** grid.

### 4. To remove specific system activity records:

a. **Select** each activity log record you want to delete.

b. From the **Actions** menu, select **Purge Selected**.

c. A dialog box displays asking if you want to remove the selected records. Click **Yes**.

### 5. To remove all activity records in the grid:

a. From the **Actions** menu, select **Purge All**.

b. A dialog box displays asking if you want to remove the selected records. Click **Yes**.

The system activity records are deleted from the log.

## Task Agent Log

Task agents handle all scheduled tasks within the Epicor ERP application. The task agent activates any program added to a recurring schedule.

Users add programs to recurring schedules through the **Schedule** drop-down lists available on programs throughout the Epicor application. Users create these schedules in the Epicor ERP application using **System Agent Maintenance**. You can review the processes the task agent ran through the event log. This log displays in the Event Log Viewer.

## Event Log Viewer

While the Task Agent runs, various events occur. These events are tracked unconditionally in the Event Log Viewer.

Multiple versions of the Task Agent Service Configuration program can be installed on the server. The event log records the activity from all these task agents and displays their activity in a single log. You use this window to organize the log by task agent and help troubleshoot issues. This topic explains how to display this window and filter the events that accumulate in the event log.

By default, this log is set to a minimum size of 10240 (10) MB. You can adjust this size by launching the Microsoft® Event Viewer® and displaying the properties for the Epicor ICE Task Agent Service. Modify the **Maximum log size** value to the size you need. Note that if you change this value to less than 10 MB, restarting the task agent service or the Task Agent Service Configuration program will cause the log size to revert back to the 10 MB default value.

**1. Launch Task Agent Service Configuration.**

**2. Click Actions > View Event Log.**

The **Event Log Viewer** displays. All the events recorded against the current task agent display in this window.



**Note** If the Task Agent stopped working and the Event Log Viewer has none or insufficient information on an event, check the Application log in the **Microsoft® Event Viewer®** for an event where the source is **Task Agent Service**.

**3. You can filter the events to only review the ones you need. To do this, click on the drop-down list next to the **equals** (=) sign; this list is below the **Level** column.**

**4. Select an option from the list. Available options:**

- **(Custom)** - Launches the **Custom Filter Selection** window.
- **(Blanks)** - Causes the grid to only display blank event records.
- **(NonBlanks)** - Causes the grid to only display records that contain values; this option filters blank records.
- **Error** - Restricts the grid to only display error messages.
- **Information** - Restricts the grid to only display information messages.
- **Warning** - Restricts the grid to only display warning messages.

**5. When you select the (Custom) option, you then enter the condition(s) against which you will filter the event log. You define these options in the Custom Filter Selection window:**

- a. Select the **Operator** you want to use for the first condition. You can use equals (=), less than (<), greater than (>), and so on.
- b. Now select the **Operard** for the condition. You can select Error, (NoBlanks), Warning, and so on.
- c. Click **Add Condition** to enter multiple filter conditions; click **Remove Conditions** to delete one or multiple filter conditions.
- d. If you select multiple conditions on the grid, you can then group them by clicking either the '**And' Group**' or the '**Or' Group**' buttons. 'And' conditions must all filter to true before the event displays; 'Or' conditions only require that one condition in the group filters to true before the event displays.
- e. Click the **Toggle** button to change a group to an 'And' or an 'Or' group.
- f. When you finish setting up the custom filter conditions, click **OK**. You return to the Event Log Viewer and the events filter using your custom conditions.

**6. To sort the events by task agent, use the **Source** column. You can click the column and sort the events in ascending or descending order. You can also click and drag the Source column into the **group by area**; all the events will then group by each task agent.**

**7. Use the **Level** column to either sort or group by the events by the event log level.**

8. You can also sort or group by the **Date and Time** recorded against each event.
9. To view the entire message for an event, click on the event row.  
The message displays in the field at the bottom of the Event Log Viewer.
10. Use the center splitter bar to resize this text window so you can see all or most of the message text.
11. Likewise, you can click the **Maximize** button to cause the Event Log Viewer to fill your screen. You can then resize the columns so you can see the data generated in each column.
12. If you need to view the new events that occurred after you opened the Event Log Viewer, click **Actions > Refresh**. This action re-fetches the event log entries.
13. When you finish reviewing the events, click the **Close** button.

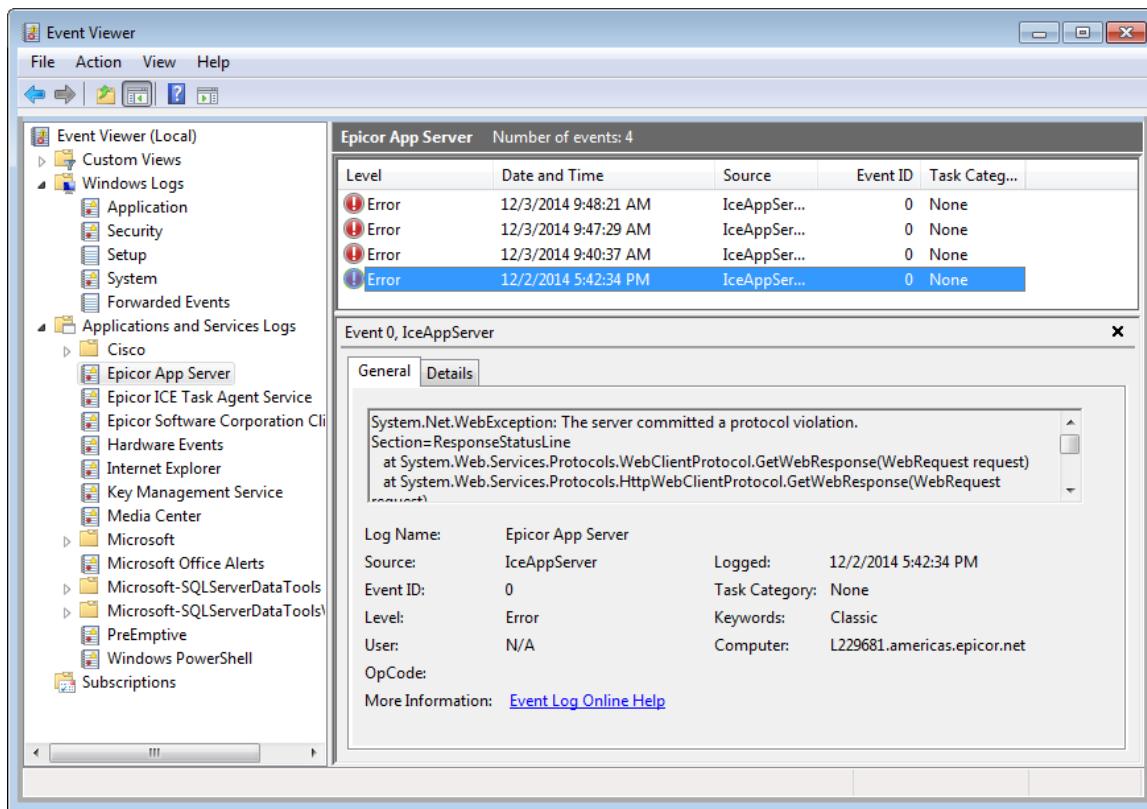
## Event Viewer

The Event Viewer is an administrative tool installed with your Windows operating system. Use this tool to review exceptions that occur outside of the Epicor ERP application.

The application server tracing log you activate within the Epicor Administration Console records business logic exceptions internal to the Epicor ERP application. For example, this log records an error when too many characters are entered in a field, a record already exists, how long it takes a business object method to run, and so on.

Any errors that occur outside of the internal business logic is recorded in the Event Viewer. Any errors you are not seeing in the application server log should display in this administrative tool. Examples of items not captured by this log include framework exceptions, security exceptions, fatal errors, and similar items.

Be sure to launch the Event Viewer to catch other problems that may slow performance. When you use the Event Viewer with the application server log, you have a complete picture of the application, server, and network issues you may be experiencing.



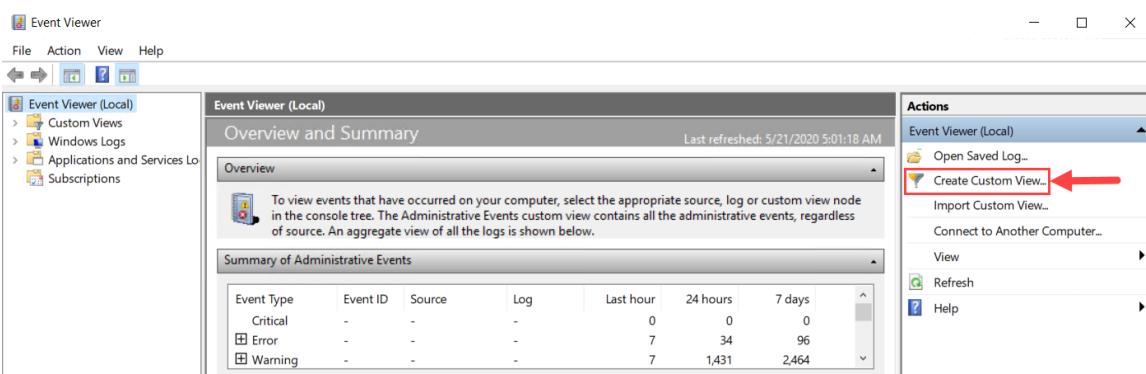
You access this Windows tool through a Windows control panel. Launch the **Administrative Tools** control panel; the **Event Viewer** displays as a shortcut. You should add this shortcut to your desktop so you can more easily launch this key tool when you need it.

## Add Custom View

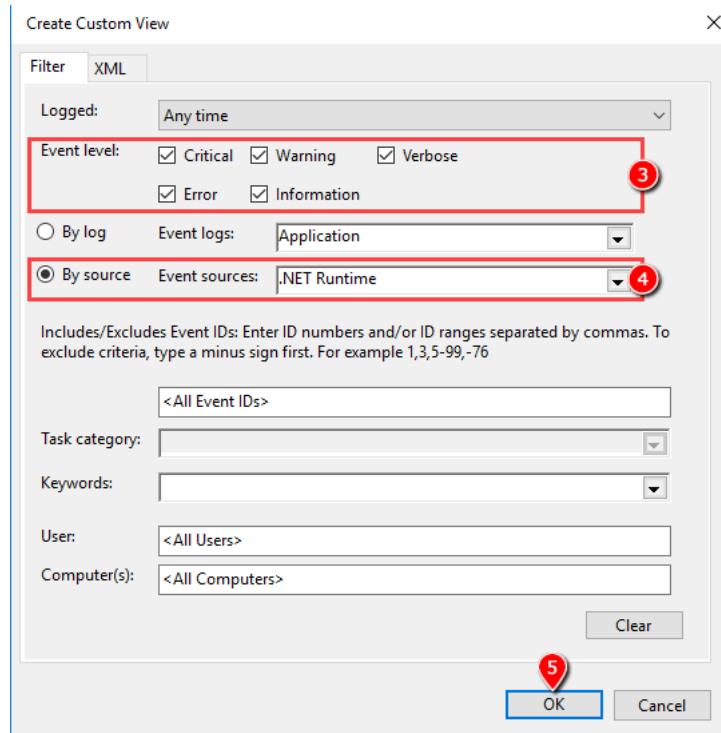
This topic explains how you can create a custom view for Epicor Client sourced events.

In some Windows versions, the **Epicor Software Corporation Client Log** that groups events originating from the application Client may not be generated automatically. If the custom Epicor Software Corporation Client Log does not get created in the MS Event Viewer®, Epicor Client events are redirected to the standard Windows application event log. In the Event Viewer, you can create a custom view folder for the **.NET Runtime** source that will include the Epicor Client events. To do this, follow the steps below:

1. Launch **Event Viewer®**.
2. On the **Actions** panel, select **Create Custom View**.

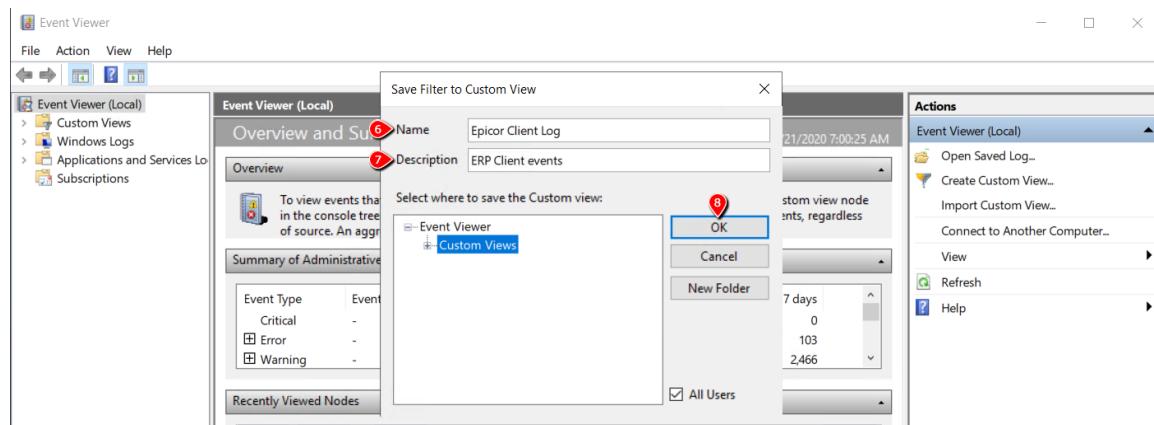


The **Create Custom View** window displays



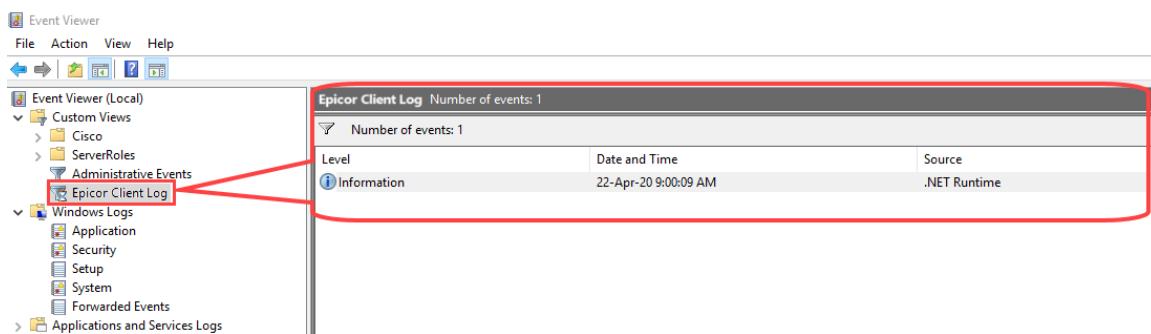
3. On the **Filter** tab, select the **Event levels** you wish to include in this view.
4. Then, select the **By source** radio button, and from the drop-down, select the **.NET Runtime** source.
5. Click **OK**.

The **Save Filter to Custom View** window opens.



6. Enter a **Name** - for example, **Epicor Client Log**.
7. Add a **Description** - for example, **ERP Client events**.
8. Click **OK**.

You can now open this custom folder to view the events generated by the Client.



**Tip** Alternately, try running the Epicor ERP as administrator by right-clicking the ERP launch icon and selecting the **Run as administrator** option. This should automatically generate the **Epicor Software Corporation Client Log** in Event Viewer.

## Server File Download

Use the Server File Download process to download a file from the Epicor server to a client directory. Download any file saved in the Server Data Directory folder, such as a log file, so that you can access it on your own computer.

Use the Server File Download functionality to review files when you don't have direct access to the server file system, such as with SaaS and Early Access. It transfers one file at a time from one of three directories on the server: Company, User, or Reports) to a client directory.



**Note** Users are not allowed to delete files from the Epicor Server Data Directory folder. Be aware that the contents of the directories are purged on a regular basis by the Epicor SaaS team.

### Download a File

Navigate to the **Server File Download** program.

**Menu Path:** System Management > Schedule Processes > Server File Download

1. In the **Directory Type** field, select one of the three directories available:
  - **User** - this will download server files of the logged user
  - **Company** - this will download company-type files - for example, multi-company or PE logging
  - **Reports** - this will download XML files for the report that is printed - normally used for crystal reports
2. Choose a file to download. Click the **Select File...** button to browse for the file. The **Open** window displays.
3. You can click on the available folders to locate the file.
4. You can also click the **Up Folder** button to return to a parent folder.
5. Once you locate the file, select it and click **Open**. The path and filename display in the **Select File** field. Notice this window also displays both the date on which this file was last modified and the size of the file.

6. Choose the client directory path where you want to save the downloaded server file. Click the **Client Path** button.  
The **Browse For Folder** window displays.
7. Select a location and click **OK**.  
The path displays for confirmation in the **Client Path** field.
8. Click **OK**.

The selected file downloads to the client directory path you defined.

# Troubleshooting

---

If you are experiencing system problems, review the topics in this section. It contains information about the most common issues and the steps you can follow to resolve these issues.

If you are unable to fix the issue, this section also describes the Support Checklist. Before you contact Epicor Technical Support, review this checklist to gather the information support needs to more quickly evaluate the issue.

## Connectivity Errors

---

This section documents some typical connectivity issues and their solutions.

### Load Balancer and Reverse Proxy Connectivity Issues

While you configure Epicor ERP application to run using a load balancer (such as **F5 Switch**) or a reverse proxy, you may receive an **Unable to Resume at this Time** error.

The specific error:

- The message with To 'net.tcp://localhost/<YourEpicorEnvironment>/Lib/SessionMod.svc' cannot be processed at the receiver, due to an Address Filter mismatch at the EndpointDispatcher. Check that the sender and receiver's EndpointAddresses agree.

For example, this **Address Filter** mismatch error may occur when the F5 Switch cannot offload Secure Socket Layer (SSL) processing from Internet Information Services (IIS). Your system needs a .WCF extension to complete the connection between SSL and IIS. You can correct this issue by activating two .WCF settings in your web.config file:

1. Using your **File Explorer** or **Windows Explorer**, navigate to the directory for the **web.config** file. For example: C:\Epicor\<YourInstallFolder>\Server
2. Open the web.config file in **Notepad** or a similar text editor.
3. Locate and uncomment this setting:

```
<extensions>
...
<!-- Uncomment this element when AddressFilter mismatch at the EndpointDispatcher happens
     <behaviorExtensions>
       <add name="AddressFilterModeAny" type="Epicor.Hosting.Wcf.AddressFilterModeAnyElement, Epicor.System, Culture=neutral, PublicKeyToken=37a5ccb872c00aec"/>
     </behaviorExtensions>
   -->
...
</extensions>
```

4. Likewise, locate and uncomment this setting:

```
<serviceBehaviors>
  <behavior>
```

```
...
<!-- Uncomment this element when AddressFilter mismatch at the EndpointDisp
atcher happens
    <AddressFilterModeAny/>-->
    </behavior>
</serviceBehaviors>
```

## 5. Save the web.config file.

The Epicor ERP application should now run as expected.

## Cannot Generate SSPI Context Error

If you receive the **Cannot Generate SSPI Context** error, you do not have a **Service Principal Name (SPN)** value defined for the Domain User Account you have selected for the **HttpsBinaryWindowsChannel** protocol binding.

If you use a built-in account with this protocol binding, the built in account automatically receives an SPN value when it is created. However custom accounts typically have more powerful security than built-in accounts. Because of this, you must manually generate an SPN value for the custom account. For example, if you select a custom account with **Kerberos** authentication, you need to manually generate the SPN number for it.

You do this by running the **setspn.exe** utility. **Setspn** is a command-line tool you activate through the Command Prompt or PowerShell windows. Review the Microsoft documentation available on the internet to learn how to run this utility.

## Insufficient Winsock Resources

While you attempt to connect to the Epicor server, you may receive the **Insufficient winsock resources available to complete socket connection initiation** error. To resolve this issue you must add or update the **MaxUserPort** value data in the registry file. .

Do the following steps:

1. Using your explorer, navigate to  
**HKEY\_LOCAL\_MACHINE>SYSTEM>CurrentControlSet>services>Tcpip>Parameters** location.
2. Search for the **MaxUserPort** parameter. If you cannot find this parameter, add it in this location.
3. Now open this parameter.  
The **Edit DWORD (32-bit) Value** dialog box displays.
4. Enter **Value Data = fffe**.
5. Click **OK**.

Your new or revised MaxUserPort registry file is saved, and this error message no longer appears.

## Database Errors

Epicor Technical Support has identified these common database issues and their solutions.

### Create Database Permission Denied

When you attempt to create a database, you receive a database permission denied error.

The error message:

- **Create database permission denied in database master.**

This error happens when you are logged into the SQL Server with an administration account that does not have the **DB Creator** server permission. Launch **Microsoft SQL Server Management Studio** and create or update the administration account so it has these permissions. The next time the user logs into SQL Server, this user can create Epicor databases without error.

### Database Size Too Small

When you try to create a new database in the Epicor Administration Console, you receive an error that the database size is too small. You then cannot create the new database.

The error message that displays:

- **MODIFY FILE failed. Specified size is less than or equal to current size.**

This error occurs because the you need to increase the size limit on the database. You do this by running a query in SQL Server Management Studio.

1. Launch **Microsoft® SQL Server Management Studio®**.

2. **Connect** to SQL Server.

3. Click the **New Query** button.

The new query displays in the center pane.

4. Enter the following script:

```
USE [master]
GO
ALTER DATABASE [model] MODIFY FILE ( NAME = N'modeldev', SIZE = 20480KB )
GO
```

5. Click the **Execute** button.

The query increases the size of the database.

Now launch the Epicor Administration Console again. You should be able to create the new database without errors.

## Index Outside Bounds of Array

While adding a database through the Epicor Administration Console, you receive an error that states the index was outside the bounds.

The specific error that displays:

- **Index was outside the bounds of the array.**

This error occurs because you are using an older version of the Epicor Administration Console. Because this tool is no longer at the same version level as the Epicor ERP application, the Epicor Administration Console cannot create a database that matches the current version number of the application.

To correct this issue, you first uninstall the Epicor Administration Console. Then reinstall the current version of this tool.

1. From the Windows Desktop, click **Start > Control Panel**.  
The **Adjust your computer's settings** window displays.
2. Select the **Programs and Features** icon.  
The **Uninstall or change a program** window displays.
3. Select the **Epicor Administration Console** icon.
4. Click the **Uninstall** button.  
A wizard displays that guides you through the uninstall process. Click through this wizard to run the uninstall program.
5. Now launch **Windows® Explorer®**.
6. Navigate to the **C:\Program Files (x86)\Common Files\Epicor Software Corporation\Epicor Administration Console** folder.
7. Delete the **Epicor Administration Console** folder.
8. Now reinstall the Epicor Administration Console. Be sure you install the most current version.
  - a. If you have installed a base version, navigate to  
**C:\Epicor\ERP10\ERP10.X.XXX\SupplementalInstalls\Administration** (Where ERP10.X.XXX is your current version).
  - b. If you have installed an update, navigate to  
**C:\Epicor\ERP10\ERP10.X.XXX\Updates\ERP10.X.XXX\SupplementalInstalls\Administration** (Where ERP10.X.XXX is your current update).
9. Launch the **setup.exe** program.
10. The install wizard displays. Click through this wizard to reinstall the **Epicor Administration Console**.
11. After you finish the installation, reboot the computer.

You should now be able to add a database through the Epicor Administration Console.

## Wrong Server Data Directory

When you first add a database to the system, be sure you enter the correct Server Data Directory on the system agent. If you enter the wrong data directory, some application processes will fail to generate data.

When you install the Epicor ERP application, the installation creates a file location on the server that receives processing data; this folder is the **EpicorData** directory. Several processes write logs and other files to this EpicorData directory. If the process cannot locate this directory file location, the process generates an error and stops running.

To make sure you have entered the correct path for the Server Data Directory, locate this file folder on the server machine. Some examples of these file directory locations:

- \\epicor\EpicorData
- C:\EPICOR\ERP10\ERP10.00.000\EPICORDATA
- C:\EpicorData

To review and update the server data directory on the system agent:

1. Navigate to **System Agent Maintenance**.

**Menu Path:** System Setup > System Maintenance > System Agent



**Important** This program is not available in Epicor Web Access.

2. Make sure the **Detail** sheet displays.

3. Review the file location that displays in the **Server Data Directory** field. Update this directory as needed.

4. Click **Save**.

Now test a process that was generating errors. The process should run as expected.

## Epicor Web Access Errors

---

This section documents errors that can occur with Epicor Web Access (EWA).

### Configurator Error

When users attempt to deploy a configurator record to Epicor Web Access (EWA), an error message displays that states the user needs to set up a valid Web Application Folder.

This error message occurs when users are in **Configurator Entry**. Users set up the configurator record. They next click the **Actions > Deploy to EWA** option. The following error message displays:

- Please set up a valid Web Application Folder and URL on the Company Maintenance form.

To correct this issue, you need to enter the correct Metadata path for the current company:

1. Navigate to **Company Maintenance**.

**Menu Path:** System Setup > Company/Site Maintenance > Company Maintenance



**Important** This program is not available in Epicor Web Access.

2. Click on the **General Settings** tab.
3. Locate the **Web Access** group box.
4. Enter the correct path in the **MetaData Output Path** field.



**Example** C:\inetpub\wwwroot\EpicorWebAccess

5. Click **Save**.
6. Instruct the user to log out and then back into the Epicor ERP application.

The user should now be able to deploy the configurator record to EWA.

## Deploy Customization Error

A user creates and deploys a customization for EWA. When the user attempts to log into the EWA interface, the following error message displays:

- Logon failure: unknown user name or bad password.

To correct this issue, you need to enter the correct Metadata path for the current company:

1. Navigate to **Company Maintenance**.



**Menu Path:** System Setup > Company/Site Maintenance > Company Maintenance

**Important** This program is not available in Epicor Web Access.

2. Click on the **General Settings** tab.
3. Locate the **Web Access** group box.
4. Enter the correct path in the **MetaData Output Path** field.



**Example** C:\inetpub\wwwroot\EpicorWebAccess

If you installed the EWA site on the same server as Epicor ERP, you enter this path:

\[MyServerName]\epicorwebaccess\

5. Click **Save**.
6. Instruct the user to deploy the customization again.
7. Now have the user log into the EWA interface.

The user should log into EWA without error. The customization should also display on the EWA interface.

## Invalid User ID

When users attempt to log into the EWA interface, they receive an Invalid User ID error message.

When this occurs, the user is unable to log into Epicor Web Access. The complete error message that displays:

- Server was unable to process request. ---> An unsecured or incorrectly secured fault was received from the other party. See the inner FaultException for the fault code and detail. ---> System error.

To correct this error, you need to update this person's user account. The account needs to have access to the Epicor Web Access client.

1. Launch Epicor ERP.

2. Navigate to **User Account Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

3. Click the **User ID...** button to find and select the user account you need to update.

4. Now click the **Options** tab.

5. Locate the **Access Options** group box.

6. Select the **Allow Epicor Web Access** check box.

7. **Save** the user account.

This user can now log into the Epicor Web Access interface.

## Logon Errors

---

This section describes some common logon errors identified by Epicor Technical Support and what you can do to resolve these issues.

### ASP.NET Impersonation Error

If users cannot log into the Epicor ERP application, it may be that ASP.NET Impersonation is running. You must disable this service.

To do this, you launch Internet Information Services (IIS) Manager. You then select the web page for your Epicor ERP installation and display the Authentication options for this site. You then disable the ASP.NET Impersonation service.

1. To launch the **IIS Manager** from your Windows desktop, click **Start**.
2. In the **Search** field, enter **IIS**.
3. **Internet Information Services (IIS) Manager** displays in the search results. Select the icon for this program. **Internet Information Services (IIS) Manager** launches.
4. From the tree view, expand the **Sites > Default Web Site** node.

5. Select the web page node for your Epicor ERP installation.  
The center pane now displays the **/[YourEpicorInstallation] Home** title.
6. Under the IIS options, double-click the **Authentication** icon.  
The **Authentication** options display.
7. Locate **ASP.NET Impersonation**. If its **Status** displays as **Enabled**, this active service is preventing users from logging into the Epicor ERP application.
8. Right-click the **ASP.NET Impersonation** node; from the context menu, select **Disable**.  
The **Status** for this Authentication service now displays as **Disabled**.
9. **Close** the Internet Information Services (IIS) Manager.

Your users should now be able to log into the Epicor ERP application.

## Cannot Log into Modern Shell

A user can no longer log into the Modern Shell interface. The user previously able to use the Modern Shell interface with no issues.

When the user attempts to log into the Modern Shell interface, the Epicor application freezes. The user has to use the Task Manager to close the application. This occurs because the user created a personalization that has an error or is not compatible with the Modern Shell interface. To correct this issue:

1. On your server machine, launch **SQL Server Management Studio**.
2. Connect with **SQL Server**.
3. Expand the **Databases** node.
4. Now expand the **[DatabaseName] > Tables** node.
5. Locate the following tables:
  - **Ice.XXXDef** (Where XXX is the user's account identifier).
  - **Ice.XXXChunk** (Where XXX is the user's account identifier).
6. Delete these personalization tables.

The user can now log into the Epicor ERP application as expected.

## Layer Verification Failure

When a user logs into a client installation, a Layer Verification Failure error message appears.

After you upgrade the Epicor ERP application, you must verify all customizations and personalizations. These modifications are interface layers that need to be synchronized with the base interface layer. When these layers are not verified, the application sees they are not synchronized and so displays this error message.

You verify customizations and personalizations through Customization/Personalization Maintenance. The verification tool can review all the custom fields and code within a selected customization/personalization or a group of customizations and personalizations. After it has finished testing the customized or personalized programs, review the Status field on the Detail sheet to see if the program passed its verification. If it did not, you can discover what caused the verification to fail on both the Warnings and Errors sheets.

To verify a group of customizations and personalizations:

1. Log into Epicor ERP using your **System Manager** user account.

2. Navigate to **Customization/Personalization Maintenance**.

**Menu Path:** System Management > Upgrade/Mass Regeneration > Customization Maintenance



**Important** This program is not available in Epicor Web Access.

3. Click the **Name...** button.

The **Customization/Personalization Search** window displays.

4. Click **Search**.

All customizations and personalizations display in the **Search Results** grid.

5. Click **Select All** and then click **OK**.

You return to **Customization/Personalization Maintenance**. Notice the customizations and personalizations display in the tree view.

6. Click **Actions > Verify All**.

7. A warning message displays indicating this process may take several minutes to complete. Click **Yes**.

The verification process reviews the customizations and personalizations. When the process is complete, you return to **Customization / Personalization Maintenance**.

8. Select a customization and review the **Detail** sheet.

9. If the **Status** field displays an **Error** value, click the **Compile/Script Errors** sheet to see what elements within the program did not verify.

10. Click the **Warnings** sheet to review any error messages that may have been generated by the selected program.

11. You can now use the **Run**, **Modify**, and **Show Custom Data** options to correct these issues. These options are all available from the **Actions** menu.

12. To verify a selected customization, click **Actions > Verify Customization**.

When all customizations and personalizations display Pass in the Status fields, the Layer Verification Failure error message no longer appears.



**Tip** If the verification error is caused by a personalization, you can also use Personalization Purge to completely remove the personalization layer.

**Menu Path:** System Management > Purge/Cleanup Routines > Personalization Purge



**Important** This program is not available in Epicor Web Access.

## Maximum Users Exceeded On License Type

When a user logs in, this person receives the "Maximum users exceeded on license type" error message. The user then cannot access the Epicor ERP application.

This error occurs because a license needs to be imported for this application server. To correct this error:

1. On your server machine, launch the **Epicor Administration Console**.

2. From the tree view, expand the **Server Management > [YourServerName] > [AppServerName]** node.
3. Right-click the **Licensing** node; from the context menu, select the **Import License File** option.  
The **Import Epicor License File** window displays.
4. Navigate to the folder location that contains the .lic file for your organization.
5. Click **Open**.  
The license file is imported and displays in the center pane. You can now activate the licences.
6. Double-click the license file.  
The **[LicenseName] Properties** window displays.
7. Click on the **Assigned Companies** tab.
8. Add companies you need to this license.
9. Now click on the **Modules** tab.
10. For each licensed module, click its **Enabled** check box.
11. Click **OK**.
12. Now from the **Actions** pane, select the **Stop Application Pool** option.
13. When the application pool stops, click the **Start Application Pool** option.

Now have the user log into the Epicor application. The user should be able to log into the system without errors.

## No License Configured for Company

When users attempt to log into the Epicor ERP application, they receive a no license configured error.

The specific error message:

- "There is no license configured for Company [CompanyName]"

This error occurs because a license need to be configured for the company. You do this by adding the company to the license within the System Administration Console.

1. On your server machine, launch the **Epicor Administration Console**.
2. From the tree view, expand the **Server Management > [YourServerName] > [AppServerName]** node.
3. Select the **Licensing** node.  
The center pane populates with the available licenses.
4. Right-click a license node; from the context menu, select **Properties**.  
The **[LicenseName] Properties** window displays.
5. Click on the **Assigned Companies** tab.
6. Enter the **Company Name** for the company.
7. Now enter the **Code** for the company.
8. Click **OK**.

Users should now be able to log into this company as expected.

## Open Exception Error

When users attempt to log into the Epicor ERP application, they receive an open exception error message.

The specific error message text that displays:

- The underlying provider failed on Open Exception.

To correct this issue, you need to grant database access to the NT Authority/Network Service. Internet Information Services (IIS) uses network credentials when it attempts to log into SQL Server. You change the application pool settings in IIS so the database uses network credentials.

1. Log into the server machine.
2. Click **Start > Administrative Tools**.  
The **Administrative Tools** window displays.
3. Launch **Internet Information Services (IIS) Manager**.
4. From the tree view, expand the server node.
5. Select the **Application Pools** node.  
The list of application pools display in the center pane.
6. Right-click the application pool you use for the application; from the context menu, select the **Advanced Settings...** option.  
The **Advanced Settings** window displays.
7. Locate the **Process Model** section.
8. Select the **Identity** setting.
9. Click the **Browse (...)** button next to this setting.  
The **Application Pool Identify** window displays.
10. Select the **Built-in account** radio button option.
11. Click **OK**.  
You return to the **Advanced Settings** window.
12. Click **OK** again.
13. Now close the **Internet Information Services (IIS) Manager**.

The user should now be able to log into the Epicor ERP application.



**Tip** If you use an SSRS server, the connection uses the LocalSystem account. This is the default user account available through the Windows operating system. If you do not use an SSRS server, the connection uses the ApplicationPoolIdentity account. This is the default user account available through Internet Information Services (IIS).

## Server Rejects Client Credentials

After a user enters a User ID and Password, the user gets a server reject client credentials error message.

The specific error message:

- "The server has rejected the client credentials"

This error occurs when users are logging into the client through either Terminal Server® or Citrix®. The application server is no longer synchronized with these systems, and so users are unable to login. To correct this issue:

1. Go to the server machine.
2. Log out of either **Terminal Server** or **Citrix**.
3. Log back into Terminal Server or Citrix.
4. Now log into the **Epicor ERP** application.

The Epicor ERP application should launch as expected.

## Printing Outages

---

Epicor Technical Support has identified some common issues that prevent users from printing reports. Review the topics in this section, as they may help you correct these printing outages.

### All Reports Have PENDING Status

Reports do not print and processes do not run. When you check the **System Monitor** and click the **Active Tasks** tab, you see all the reports and processes have the PENDING status. This situation is caused by several conditions that range from temporary memory spikes to deeper system issues.

You can try to activate the reports/processes by first stopping and restarting the task agent service. If that doesn't activate the reports/processes, you next try stopping and restarting the application pool.

1. Go to your server machine.
2. Launch the **Epicor Administration Console**.
3. From the tree view, expand the **Server Management > [YourServerName] > [YourApplicationServer]** node.  
The center pane displays the details for your selected application server.
4. Click the **Task Agent Configuration** button.  
The **Task Agent Service Configuration for [VersionNumber]** window displays.
5. To stop the task agent service, click **Actions > Stop Service**.
6. A message displays indicating the service is stopped. Click **OK**.  
The task agent is no longer running; the Task Agent Service Configuration window is empty.
7. When you are ready to activate the task agent again, click **Actions > Restart Service**.

8. A message displays stating the service is restarted. Click **OK**.  
The task agent details appear on the **Task Agent Service Configuration for [VersionNumber]** window. A green icon also displays, indicating the task agent is running.
  9. Now attempt to run a report.  
If the report prints or previews as expected, the issue is resolved. However if the report again stays on the **System Monitor > Active Tasks** tab with the PENDING status, continue with the next steps.
  10. Close the **Task Agent Service Configuration for [VersionNumber]** window.
  11. Once again from the **Epicor Administration Console**, use the tree view to highlight the application server.
  12. From either the **Action** menu or the **Actions** pane, select **Stop Application Pool**.
  13. You are asked if you are sure you want to terminate all active user sessions and prevent users from logging in. Click **Yes**.
  14. A dialog box displays indicating the application pool is stopped. Click **OK**.
  15. From either the **Action** menu or the **Actions** pane, select **Start Application Pool**.
-  **Tip** You can also right-click the application server to display both the Stop and Start options on a context menu.
16. A dialog box displays indicating the application pool is started. Click **OK**.
  17. Now attempt to run a report again.  
The report should print or preview as expected.

If you continue to have issues, contact **Epicor Technical Support**. They can help you stop and restart other services that may activate the pending reports and/or processes.

 **Tip** If this issue frequently occurs, consider setting up another application server that just runs processes and/or reports. This moves the load off to an application server that has more resources to handle the processes or reports. For more information, review the **Performance Tuning Guide**; the **Load Distribution** section describes how to assign specific report/processes to a different application server. To navigate to this guide:

- **System Management > Working With System Management > Performance Tuning Guide**

## Can Preview, Cannot Print

You can display the report in the Print Preview window, but the report does not print on the SSRS printer. The Event Viewer displays the following error message:

- System error has occurred! /n/rReport Name:/reports/<ReportName>/SOForm/n/rError: The request failed with HTTP status 401: Unauthorized.

This error occurs because the Epicor SQL Report Monitor Service uses the LocalSystem account. This account does not have access to the network and so it cannot connect to the SSRS printer. You need to change the user account on the Epicor SQL Report Monitor Service to a network domain user account that has local administrator permissions.

 **Important** The SSRS printer also needs to be installed on the EpiSSRSPortal server. If this printer is not installed on this server, the Event Viewer will display an **Invalid Printer** error.

To correct this issue:

1. Log into your server machine that contains the Epicor ERP application server.
2. Launch **Internet Information Services (IIS) Manager**.
3. From the tree view, select the **Application Pools** node.
4. Now select the application pool for your Epicor ERP application.
5. From the **Actions** pane, select the **Advanced Settings...** option.  
The **Advanced Settings** window displays.
6. Locate the **Identity** property; notice it displays the **LocalSystem** value.
7. Change this property to use a valid domain service account.
8. Click **OK**.
9. Now from the **Actions** pane, **Stop** the application server.  
The application server stops.
10. To activate the application server again, click the **Start** option.
11. Launch the **Epicor Administration Console**.
12. From the tree view, expand the **Server Management** node and the **[YourServerName]** node. Select your Epicor ERP application server.
13. Click the **Task Agent Configuration** button.  
The **Task Agent Service Configuration for [VersionNumber]** window displays.
14. Select the **Actions > Stop Service...** option.
15. After the task agent stops, select the **Actions > Restart Service...** option.  
The task agent re-activates.
16. Log into the Epicor ERP application and test print an SSRS report.

## Cannot Find Report

When users try to run an SSRS report, they receive an error message that states the application cannot find the report. It indicates the folder does not have any reports in it.

This error happens because the application server is not pointing to the correct report folder. You need to update the application server to connect to a valid SSRS root folder. To correct this issue:

1. Access your server machine.
2. Launch the **Epicor Administration Console**.
3. From the tree view, expand the **Server Management > [YourServerName]** node.
4. Select your application server.

When the Epicor Administration Console connects with this application server, its connection information displays in the center pane.

5. Now right-click the application server; from the context menu, select **Application Server Configuration**.



**Tip** You can also click the Application Server Configuration option on the Actions pane.

The **Application Server - Site Properties** window displays.

6. Select the **Reporting Services** tab.

7. Enter the correct **SSRS Root Folder** location.

This directory defines the root folder location where you will deploy the reports. For example, enter Epicor if you want the reports to deploy to the Epicor/Reports folder. If you leave the field blank, this root folder will be the directory that contains the report server home page file; the reports will deploy to the /Reports sub-folder in this directory.

8. Click **Deploy**.

The application server updates with your new root folder location.

Users can now print and preview SSRS reports.

## Cannot Print to a Client Printer

When you try to print to a client printer (instead of a server printer), you receive the following error message:

- Server Side Exception The request failed with HTTP status 404: Not Found. Exception caught in: Epicor.ServiceModel

This error occurs because the Reporting Services properties are not set up correctly for the application server. To resolve this issue:

1. Log into your server machine.

2. Launch the **Epicor Administration Console**.

3. From the tree view, expand the **Server Management** node and the **[YourServerName]** node. Select your Epicor ERP application server.

4. From the **Actions** pane, select the **Application Server Configuration** option.

The **Application Server - Site Properties** window displays.

5. Click the **Reporting Services** tab.

6. Review the **SSRS Base URL** field. If this field is blank, enter the base URL value in this field. However if this field already displays a URL value, verify whether this value is correct.

7. Now review the **SSRS Root Folder** field. If this field is blank, enter the folder value in this field. However if this field already displays a root folder value, verify whether this value is correct.

8. Click **Deploy**.

The application server updates with these updated SSRS values.

9. Now log back into your Epicor ERP application.

10. Test a report by sending it to the client printer.

The report should print as expected.

## CREATE TABLE Permission Error

A report does not print. When you launch the System Monitor and click the Reports tab, the report instance displays the following error message:

- Program Ice.Services.Lib.RunTask raised an unexpected exception. RunTask: CREATE TABLE permission denied in database '<DatabaseName>'.

You can correct this issue by changing a value in Company Maintenance:

**1.** Log into the Epicor client that has the issue. Be sure you log in with a system manager account.

**2.** Navigate to **Company Maintenance**.

**Menu Path:** System Setup > Company/Site Maintenance > Company Maintenance



**Important** This program is not available in Epicor Web Access.

**3.** Select the **Email and Reporting** tab.

**4.** Clear (de-select) the **Override Defaults** check box.

**5.** Click **Save**.

**6.** Log out of the Epicor client application.

**7.** Log back into the Epicor client application.

**8.** Run the report.

The report should now print from this client. However if you still get the same error, log into your server machine. Launch the **Epicor Administration Console** and recycle your IIS application pool.

## LOB Data Exceeds Maximum

When you attempt to print an SSRS report, the following error message displays in the Event Viewer:

- Length of LOB data (94960) to be replicated exceeds configured maximum 65536. Use the stored procedure sp\_configure to increase the configured maximum value for max text repl size option, which defaults to 65536. A configured value of -1 indicates no limit, other than the limit imposed by the data type. The statement has been terminated.

SSRS displays this error message because the report output contains data larger than its maximum allowed value setting. You correct this issue by increasing the Max Text Replication Size value in Microsoft® SQL Server Management Studio® :

**1.** Log into the server machine.

**2.** Launch **SQL Server Management Studio**.

**3.** **Connect** to the server.

**4.** From the tree view, select the top **[YourServerName]** node.

5. Right-click this node; from the context menu, select **Properties**.  
The **Server Properties - [YourServerName]** window displays.
6. From the **Select a page** pane, select the **Advanced** node.
7. Locate the **Max Text Replication Size** property; change this value to 2000000.
8. Click **OK**.
9. **Save** your changes.
10. Exit **SQL Server Management Studio**.
11. Now log into the Epicor ERP application.
12. Run the report that generated the error. Be sure you use the same parameters that caused the report to pull in the large amount of data.

The report should run without displaying the error message.

Microsoft has published articles that describes this issue. For further information:

- <http://www.gfi.com/support/products/Error-ERROR-DAL-UploadMessageSourceFailed-is-found-in-the-Windows-Event-Logs>
- [https://msdn.microsoft.com/en-us/library/ms186225\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms186225(v=sql.105).aspx)

## Logon Fails for Execution Account

An SSRS report does not print. When you check the System Monitor, you see the following error:

- Program Ice.Services.Lib.RunTask raised an unexpected exception with the following message: RunTask: System.Web.Services.Protocols.SoapException: The report server has encountered a configuration error. Logon failed for the unattended execution account.

This error happens because when SSRS was configured, a domain user account was selected as the execution account. The password for this domain user account has now changed, causing the SSRS login to fail.

1. Find out the new password for the domain user account.
2. Log into the server machine.
3. Launch the **Reporting Services Configuration Manager**.
4. Click the **Connect** button.
5. From the **Connect** pane, select the **Execution Account** node.  
The **Execution Account** pane displays. The domain user account appears with the old password.
6. Select the **Specify an execution account** check box.
7. Enter the new **Password**.
8. Enter this password again in the **Confirm Password** field.
9. Click **Apply**.
10. Now on the **Connect** pane, select the top **[ServerName]\MSSQLSERVER** node.  
The **Report Server Status** pane displays.

11. Click the **Stop** button.
12. Now click the **Start** button.
13. Exit the **Reporting Services Configuration Manager**.
14. Log into the Epicor ERP application.
15. Test print a report.

The report should print as expected.

## Permissions Granted Error

Users are unable to print any SSRS reports. When you check the ICE Task Agent Service event log, you see the following error:

- The permissions granted to user 'Domain\ApplicationServer\$' are insufficient for performing this operation.

This error occurs when the Epicor ERP application server is installed on a separate server from Microsoft SQL Reporting Services (SSRS), and the Epicor ERP application server is linked to an application pool that uses a LocalSystem identify. Because SSRS is installed on a different server, SSRS cannot authenticate the LocalSystem account across both servers.

1. Log into your server machine that contains the Epicor ERP application server.
2. Launch **Internet Information Services (IIS) Manager**.
3. From the tree view, select the **Application Pools** node.
4. Now select the application pool for your Epicor ERP application.
5. From the **Actions** pane, select the **Advanced Settings...** option.  
The **Advanced Settings** window displays.
6. Locate the **Identity** property; notice it displays the **LocalSystem** value.
7. Change this property to use a valid domain service account.
8. Click **OK**.
9. Now from the **Actions** pane, **Stop** the application server.  
The application server stops.
10. To activate the application server again, click the **Start** option.
11. Launch the **Epicor Administration Console**.
12. From the tree view, expand the **Server Management** node and the **<YourServerName>** node. Select your Epicor ERP application server.
13. Click the **Task Agent Configuration** button.  
The **Task Agent Service Configuration for <VersionNumber>** window displays.
14. Select the **Actions > Stop Service...** option.
15. After the task agent stops, select the **Actions > Restart Service...** option.

The task agent re-activates.

16. Log into the Epicor ERP application and test print an SSRS report.

The SSRS report should now print as expected.

## Printer Setting No Printing Error

When you select the Standard - SSRS report style on a report window and click Print, a dialog box displays with this message:

- Printer Setting: Printer: No Printing.

This message indicates that you do not have an SSRS printer configured for the Epicor ERP application. To correct this issue:

1. Launch **Printer Maintenance**.

**Menu Path:** System Management > Reporting > Printer Maintenance



**Important** This program is not available in Epicor Web Access.

2. Either click the **Printer ID...** button to find and select an existing printer record or click **New** to create a new printer record.



**Important** This printer needs to have access to the server where the **EpiSSRSPortal** website is installed.

3. Select the **SSRS Printer** check box.

4. Close **Printer Maintenance**.

5. Log out of the Epicor ERP application.

6. Log into the Epicor ERP application.

7. Return to the report and select the **Standard - SSRS** report style.

8. **Print** the report.

The error message no longer displays.

## Print Process Times Out

When you attempt to print a report, you receive the following error message:

- Program Ice.Services.Lib.RunTask. The operation has timed out

This indicates your system has run out of resources. To resolve this issue, stop and restart the application pool for the application server:

1. Log into your server machine.

2. Launch **Internet Information Services (IIS) Manager**. Click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

**3.** Select the **Application Pools** node.

The center pane displays the application pools available on your system.

**4.** Right-click on the application pool for your application server; from the context menu, select **Stop**.

**5.** Wait ten seconds, and then right click the application pool for your application server again; from the context menu, select **Start**.

 **Tip** Optionally you can also stop and restart the application server within the Epicor Administration Console. To do this, expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Stop** and **Start** options.

**6.** Log into the Epicor ERP application.

**7.** Test print a report.

The report should print as expected.

## Remote Name Does Not Resolve

When you attempt to print a report, you receive the following error:

- Program Ice.Services.Lib.RunTask raised an unexpected exception with the following message: RunTask: The remote name could not be resolved: '<RemoteName>'.

This error occurs because the server that runs SSRS has been renamed since you last configured the application server. You need to update this name on the application server.

**1.** Make sure all users are logged out of the Epicor ERP application.

**2.** Now log into your server machine.

**3.** Launch the **Epicor Administration Console**.

**4.** From the tree view, expand the **Server Management** node and the **<YourServerName>** node. Select your Epicor ERP application server.

**5.** From the **Actions** pane, select the **Application Server Configuration** option. The **Application Server - Site Properties** window displays.

**6.** Click the **Reporting Services** tab.

**7.** Update the **SSRS Base URL** field with the correct URL and server name.

**8.** Click **Deploy**.

This process updates the application server with the new server name.

**9.** Test a report. It should print as expected.

**10.** Users may now log back into the Epicor ERP application.

## Server Printing Fails; No Error

A report does not print on a server printer, but no error message displays in the client log, the server log, or the Event Viewer. The System Monitor also indicates the report printed complete.

This issue happens because the printer driver is not completely installed. You can fix this by first creating the port and then separately installing the printer.

1. Log onto the server machine.
2. Launch the **Print Management** console.
3. Expand the **Print Servers** node and **[YourServerName]** application server node.
4. Right-click the **Ports** node; from the context menu, select the **Add Port...** option.  
The **Printer Ports** window displays.
5. From the **Available port types**, select the **Standard TCP/IP Port** option.
6. Click the **New Port...** option.  
The **Add Standard TCP/IP Printer Port Wizard** displays.
7. Click **Next**.
8. Enter the **Printer Name or IP Address** for the SSRS printer.
9. Now enter the **Port Name** for the port the system will use to connect to this printer.
10. Click **Next**.
11. Review the options you selected on the wizard. Click the **Back** button to make any changes you need.
12. Click **Finish**.
13. Now re-install the printer.
14. When the print installer asks for the **Port Name**, enter a different name. You will change this value later.
15. Return to the **Print Management** console.
16. Now from the tree view, select the **All Printers** node.  
The printers available in your system display in the center pane.
17. Right-click the server printer; from the context menu, select the **Properties...** option.
18. Click the **Ports** tab.
19. Select the **[PortName]** check box for the port you wish to use with this server printer.
20. Click **OK**.

You should now be able to print reports on the server printer.

## SSRS Style Does Not Display

You have set up the Epicor ERP application to only print SSRS reports. However when you attempt to print an SSRS report, the Report Style drop-down list does not display the Standard - SSRS option.

This happens because your current company is not set up to only print SSRS reports:

1. Launch **Company Maintenance**.

**Menu Path:** System Setup > Company/Site Maintenance > Company Maintenance



**Important** This program is not available in Epicor Web Access.

2. Select the **Email and Reporting** tab.
3. From the **Allowed Report Style** drop-down list, select **SSRS Only**.
4. Click **Save**.
5. Exit **Company Maintenance**.
6. Log out of the Epicor ERP application.
7. Log back into the Epicor ERP application.
8. Launch a report window.
9. Click on the **Report Style** drop-down list.

The Standard - SSRS report option displays.

## Support Checklist

---

Epicor Technical Support can resolve most issues that occur with your Epicor ERP application. However to more efficiently resolve a problem, the support analysts need detailed information about your issue and your overall system.

You can significantly shorten how long it takes Epicor Technical Support to review and analyze your issue by first eliminating its potential causes. By following a series of tests, you verify whether a customization or a Business Process Management (BPM) directive is the source of the problem. If a customization or a BPM directive is the cause, you may be able to resolve the issue without contacting support.

However if these tests do not resolve your issue, you need to contact Epicor Technical Support. Before you call and/or email, you gather a series of logs and system files. You then compress these files into a single archive (.zip or .rar) file. Send this file to Epicor Technical Support as an email attachment or upload it to the Epicor FTP site. You should also make sure you have thoroughly documented the issue by providing details about your system and the steps required to duplicate the issue. By gathering this information before you contact support, you will reduce the number of calls and emails required to thoroughly explore and resolve your issue.

### Support Checklist Tasks

The Support Checklist is a two part process where you first eliminate any potential sources of slow performance. If you eliminate these sources and the performance issue continues, you then prepare to submit a support call by gathering system information and logs.

#### Eliminate Potential Sources

Checklist Item	Task to Complete
Check Customizations	Repeat performance issue steps by using the Base form of the program(s).
Disable BPM Directives	Shut off BPM processing and repeat performance issue steps.

Checklist Item	Task to Complete
Recompile BPM Directives	Recompile all BPM Directives to verify these directives are up to date.

If you complete these tasks and the performance issue continues, you next pull together the information for the support call.

### Gather System Information and Logs

Gather the following information and place it within a central folder.

Checklist Item	Task to Complete
Create the Support Folder	Create a new <b>EpicorSupport</b> folder. As you copy system files and generate server logs, place them in this central folder.
Document Affected Program(s)	Record each program affected by the issue. Be sure that when you create the support call, the affected programs are clearly identified at the beginning of the call.
Gather Main Details	Create a document that contains your <b>Site ID, Company Name, Call Number</b> , and the <b>Epicor Version</b> .
Gather Issue Details	Answer a series of questions about the issue and create the steps to duplicate. If the issue generates an error, save the error message log.
System Information	Run the <b>msinfo32</b> command and save the results to a central folder.
Application Server Information	Capture detailed information about each application server.
Configuration Files	Copy the web.config an app.config file for the Epicor ERP application.
Task Agent and Setup Data	Compress the <b>Epicor Task Agent Service [CurrentVersionNumber]</b> folder and any <b>Setup Configuration</b> folders.
Event Viewer Files	Pull together files generated by the Windows® Event Viewer®.
Generate Server Logs	Activate server logs and select the details you need to track the performance issue.
Generate Client Logs	Activate client logs and select the details you need to track the performance issue.
Capture Logs	Run the Log Capture feature in the Performance and Diagnostic Tool to place both client and server logs into the EpicorSupport folder.

After you have finished gathering this information, you are ready to contact Epicor Technical Support. Create the support call and send the files you gathered to Epicor Technical Support for review.

The following series of topics describe each Support Checklist step in detail. Be sure to follow these steps to ensure you are gathering the correct information.

### Eliminate Potential Sources

Do the following series of tests to verify this issue occurs in the base Epicor ERP application. Through these tests, you may discover the source of the issue is a customization, personalization, or a Business Process Management (BPM) directive.

Before you do these tests, be sure to log into the Epicor ERP application through a user account that has customization privileges. If you need, launch User Account Security Maintenance to find and update a user account with these rights.

1. Navigate to **User Account Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

2. Find the user account you wish to update.
3. Select the **Options** sheet.
4. Select the **Customize Privileges** check box.
5. Now select the **BPM Advanced User** check box.
6. Save the user account.
7. Log out of the Epicor ERP application.
8. Next log into the Epicor ERP application using this account.

## Check Customizations

For the first test, verify whether this issue is caused by a customization or a personalization of the base form.

**1. Activate Developer Mode:**

- If you use **Classic Menu** interface, from the **Main Menu** click **Options > Developer Mode**.
- If you use **Modern Home Page** interface, activate this mode either from the Menu by clicking the **Settings** tile and selecting **Developer Mode** in the **General Options** group, or by moving your mouse pointer over the bottom of the screen and click the **Developer Mode** wrench icon on the **Application Bar**.
- If you use **Kinetic Home Page** style interface, from the **Overflow** menu in the top right corner of the home page, select **Developer Mode** from the list.



**Note** You can also press **Ctrl + Shift + D** to activate Developer Mode.

**2. Launch the program that is causing the error.**

The **Select Customization** window displays.

**3. Select the **Base Only** check box.**

**4. Click **OK**.**

**5. Duplicate the steps that cause the issue.**

- a. If the issue still appears, the customization or personalization is not causing the problem. Shut off **Developer Mode** and move onto the **Disable BPMs** test.
- b. If the issue does not appear, the customization or personalization is causing the issue. Contact the person who created the customization/personalization to fix the error.

## Disable BPM Directives

You next verify whether a Business Process Management (BPM) directive is causing the issue.

**1. Log into your server machine.**

2. Using **Windows® Explorer®**, navigate to the web site directory that contains the application server for the system you are testing. For example, navigate to **c:\inetpub\wwwroot\Epicor10**.
3. Open the **Server** subfolder.
4. Copy the **web.config** file and paste it into a separate directory. You can then restore this original file later.
5. Now return to the **Server** subfolder and open the original **web.config** file in **Notepad** or a similar text editor.
6. Search for the **customizationSettings disabled="false"** setting.  
This disables all BPM processing within the Epicor ERP application.
7. Change this setting to the "**true**" value.
8. Save your changes.
9. To activate this change, you need to recycle the application pool. Launch the **Epicor Administration Console**.
10. Expand the **Server Management** node.
11. Right-click the application server icon; from the context menu, select **Recycle IIS Application Pool**.
12. A message displays asking if you are sure you want to recycle the application pool; click **Yes**.
13. Return to the Epicor ERP application.
14. Once again, duplicate the steps that cause the issue.
  - a. If the issue still appears, BPM directives are not causing the issue. Return to the server machine and reactivate BPM processing by changing the web.config setting back to **customizationSettings disabled="false"**. You have now eliminated the possibility that the error is caused by either a customization or a BPM directive, and you should start preparing the data required for the support call.
  - b. If the issue does not appear, you next must verify whether your BPM directives need to be recompiled. This may resolve the issue. Move onto the next **Recompile BPMs Directives** test.

## Recompile BPM Directives

The issue may be caused because your BPM directives are out of date. By recompiling them, you update the BPM directives to match the current version.

1. Log into the **Epicor ERP** application.
2. Navigate to the **Directive Update** program.

**Menu Path:** System Management > Business Process Management > Directive Update



**Important** This program is not available in Epicor Web Access.

3. Click the **Directive Recompile Setup** tab.
4. Select the **Both outdated and up-to-date directive** check box.

5. Select the **Refresh Signatures** check box.
6. Click the **Start Recompile** button.  
A dialog box displays indicating the BPM directives are recompiled.
7. Once more, duplicate the steps that cause the issue.
  - a. If the issue still appears, you have eliminated both customizations and BPM directives as the source of the issue. You next should gather the information Epicor Technical Support needs to analyze the issue. Move onto the next **Main Details** topic.
  - b. If the issue does not appear, recompiling the BPM directives may have corrected the issue. To make sure, try recompiling the BPM directives again in a test environment for the live database. If the issue still doesn't appear, the issue is resolved. However if the issue appears again, gather the information and files you need for the support call.

## Identify Program

Be sure you determine the program or programs affected by the issue. If multiple programs are affected, create a file that contains this information for later reference.

Documenting the specific programs affected by the issue is a crucial checklist task. Be sure you keep track of which programs are experiencing issues, as you will need to prominently list them at the beginning of your support call.

## Main Details

To begin preparing your support call, gather these primary details. Be sure to have this information available at the beginning your call or email.

1. **Site ID** -- The identifier for your Epicor support account. Epicor Technical Support can then verify whether you are on a maintenance plane.
2. **Company Name** -- The name of your organization. This will help support analysts check on previous calls from the same company.
3. **Call Number** -- If you are contacting support about an existing issue, include the call number from the previous call. The support representative can then look up the history for this call.
4. **Epicor Version** -- Include the exact number for the version of the Epicor ERP application you use. For example: 8.03.400, 9.05.700, 10.1.300, and so on.

## Save Error Message Log

If the issue causes an error message to display, be sure to save the log that generates with the error message.

Error messages display in a dialog box. This dialog box has options you use to save the error message log. To display and save the error message log:

1. In the error message dialog, click **Copy**.  
The error log is added to the clipboard.



**Note** This action also adds some system information to the error log. This system information includes:

- **AppServer Connection** - specifies the application server address and the ERP instance - for example, **net.tcp://EpicorServer/ERP102700**.
- **Form Name** - specifies the name of the ERP program the error occurred in - for example, **Sales Order Entry**.
- **Customization Name** - specifies the name of the customization layer applied to the current program, if any.
- **Menu ID** - specifies the menu ID of the ERP program - for example, **OMMT3001**.
- **Software Version** - specifies the ERP version - for example, **10.2.700.3**.

2. Open a text editor like **Notepad** or a similar text editor.

3. **Paste** the error message log.

The error message and related system information now display in the text editor.

4. **Save** the error message log.

You now have an error message file you can send to Epicor Technical Support.

## Issue Details

You next need to thoroughly describe the issue.

Be sure you avoid vague explanations by specifically documenting the issue. Some examples of vague and specific issue explanations:

- **Vague:** Epicor 10 is slow.
- **Specific:** Sales Order Entry is always slow. I have used this program several times, and it always takes a long time to process orders. I have traced the performance times in the attached client log.
- **Vague:** At 7 am, everything slows down.
- **Specific:** When we run the Master Update process in Sales Order Entry, this process is consistently taking 15 seconds or more to run. The same thing happens when we run the Customer Shipment Entry > Master Update process; these calls take 20 seconds or more. I've attached the server trace log from all our application servers for your review.
- **Vague:** We aren't able to print anything.
- **Specific:** We are repeatedly unable to print Sales Order Acknowledgments and AR Invoices. Each time we have attempted to print these reports, I have run the client trace log. These client log files are attached.

To specifically document these issues, answer these questions:

1. When did the issue start?
2. Has the Epicor ERP application always have this issue, or did it start after a change was made to the application?
3. When was the last time you saw this issue?
4. Does this issue affect a single user, a group of users who work in the same area (for example, shop floor users), or all users?
5. Does the issue happen on multiple workstations, or does it just happen for a specific user?

**6.** What is the specific program or programs affected by the issue. Be sure to indicate whether this is an issue with Job Entry, MRP Processing, Sales Order Entry, and so on.

**7.** What are the steps to duplicate the issue?

If you only need a few short steps to reproduce the issue, just send those few steps. For example:

- When I save an existing record in Part Maintenance, the error message I included in this email displays.

However if the issue requires a more complex series of steps, use the **Steps Recorder** to record the exact steps to reproduce the issue. The next topic describes how you use this utility to record step-by-step information.

## Record Steps to Duplicate

The Steps Recorder is a Windows utility that records the steps required to duplicate an issue. It also saves screen captures of each step, so Epicor Technical Support can then review these screen captures.

This utility was introduced in the **Windows 7** and **Windows 2008R2** versions.

- 1.** Before you begin, you should create a **EpicorSupport** folder. You will place the files and logs you gather in this central folder.
- 2.** Log into the Epicor ERP application.
- 3.** Now click **Start**.
- 4.** In the **Search** field, type in **psr**.
- 5.** From the search results, select **Steps Recorder**.  
The Steps Recorder displays.
- 6.** Click the **Down Arrow**; from this drop-down list, select **Settings**.
- 7.** Change the **Number of recent screen captures to store** value to **99**.
- 8.** Click **OK**.
- 9.** Now click the **Start Record** button.
- 10.** Perform the steps that cause the issue.



**Tip** As you perform your steps, a red dot will flash once in a while. This indicates the Steps Recorder is tracking your steps.

- 11.** When you finish, click **Stop Record**.

The **Save As** window displays. When you save this file, you create a compressed file to send to support.

- 12.** Navigate to the directory where you are saving the support files.

- 13.** For the **File name**, enter **StepsToReproduce**.

- 14.** Click **Save**.

The **StepsToReproduce.zip** file now displays in your support folder.

## Gather System Data

You next gather information on how your Epicor ERP environment is configured. You do this by locating a series of system files, copying them, and then compressing them.



**Tip** If you haven't already done so, create an **EpicorSupport** folder. As you copy system files and generate server logs, place them in this central EpicorSupport folder.

### System Information

Next gather the following information about your Epicor application server and Internet Information Services (IIS).

1. Log into your server machine.
2. Click **Start > Run**.  
The **Run** window displays.
3. Enter **msinfo32**.
4. Click **OK**.  
The **System Information** window displays.
5. Click **File > Export**.  
The **Export As** window displays.
6. Find and select the **EpicorSupport** directory.
7. Click **Save**.

The file that contains your system information is saved to this location.



**Important** If your Epicor ERP application and SQL Server are on the same machine, you only need to do these steps once. If these applications are on different machines, repeat these steps on each machine.

### Application Server Information

Next capture the following information about each application server.

1. On the machine that contains the application server, launch the **Windows® PowerShell®**.
2. At the command prompt, enter **import-module WebAdministration** and press **<Enter>**.
3. Next enter **IIS** and press **<Enter>**.
4. For this next command, enter Epicor Site ID and Server Name in the designated parts of the command statement. Enter **Backup-WebConfiguration -Name: [SiteId]\_[ServerName]** and press **<Enter>**.
5. Navigate to the **C:\windows\system32\inetsrv\backup** directory.
6. Compress the **[SiteId]\_[ServerName]** folder.
7. Place the compressed file in the **EpicorSupport** directory.

8. Now navigate to the **C:\inetpub\logs\LogFiles** directory.
9. Compress the **W3SVC1** folder.
10. Paste the **W3SVC1** archive in the **EpicorSupport** directory.
11. If you have multiple application servers, repeat steps 8-10 to create archives for each W3SVC1 folder. Be sure to identify which archive belongs to which specific application server.

## Configuration Files

Copy the web.config an app.config file for the Epicor ERP application.

1. To find where the web.config file is located, launch the **Epicor Administration Console**.
2. Expand the **Server Management** node.
3. Now launch the **Application Server Configuration** window. You can do this in the following ways:
  - a. Right-click the **[ApplicationServer]** node; from the context menu, select **Application Server Configuration**.
  - b. From the **Actions** pane, select **Application Server Configuration**.
  - c. Click the **Action** menu; select **Application Server Configuration**.

The **Application Server - Site Properties** window displays.

4. Navigate to the **Application Server > Application Server Settings** sheet.
5. Review the directory path that displays in the **Web Site Directory** field.
6. Use **Windows® Explorer®** to navigate to this directory.
7. Copy the **web.config** file.
8. Paste the web.config file in the **EpicorSupport** directory.
9. Now copy the app.config file. Navigate to the **C:\Epicor\<YourEpicorVersion>\Server** directory.
10. Copy the **app.config** file.
11. Paste the app.config file in the **EpicorSupport** directory.

## Task Agent and Setup Data

Now gather the information support needs for the task agent and any additional setup configuration information.

1. Launch **Windows® Explorer®**.
2. Navigate to the **C:\Program Files (x86)\Epicor Software** directory.
3. Compress the **Epicor Task Agent Service [CurrentVersionNumber]** folder.
4. If any **Setup Configuration** folders display in this folder, compress them as well.

5. Place these .zip files in your **EpicorSupport** directory.

## Event Viewer Files

Now gather files generated by the Windows® Event Viewer®.

1. Log into your server machine.
2. Launch **Windows® Explorer®**.
3. Navigate to the **%SystemRoot%\System32\Winevt\Logs\** directory.
4. Copy the following files and place them in your **EpicorSupport** directory:
  - **Application.evtx**
  - **Epicor App Server.evtx**
  - **Epicor ICE Task Agent service.evtx**
  - **EpiSSRS.evtx**
  - **System.evtx**
5. Compress these files; name the archive file **EventViewerFiles.zip** or **EventViewerFiles.rar**.

## Gather Application Data

You next gather performance data from the Epicor ERP application. You do this by generating client (UI Trace) logs and server logs. You also capture system log information.

### Generate Client Logs

You can generate client (UI Trace) logs either by activating them on a user account or by directly activating them on the client installation.

1. To activate the client (UI Trace) log through a user account:

- a. Launch **User Account Security Maintenance**.

**Menu Path:** System Setup > Security Maintenance > User Account Security Maintenance

- b. On the **Detail** sheet, click the **User ID...** button to find and select the **Manager** user account.
- c. Click on the **Tracing** sheet.
- d. Select the **Enable Trace Logging** check box.
- e. Select the tracing options you need.
- f. Click **Save**.

The next time a user logs in with this account, the client (UI Trace) log will generate.

2. To activate the client (UI Trace) log directly on a client:

- a. When you run the application using the **Classic Menu** interface, you activate the trace log from the Main Menu. Click **Options > Tracing Options**.

- b. When you run the application using the **Modern Home Page** interface, you can activate the trace log by clicking the **Down Arrow** at the bottom of the window. From the toolbar, click the **Tracing Options** button. Likewise from the Modern Shell interface, you can activate the tracing log from the **Home** menu. Click the **Settings** tile and the **General Options** setting. Select **Tracing Options**.
- c. When you run the application using the **Kinetic Home Page** interface, you can activate the trace log from the **Overflow** menu. Expand the menu and select **Tracing Options**. Alternately, from the home page, click the **User** icon in the bottom left corner of the window and select **More Settings**. Then from **General Settings**, select **Tracing Options**.
- d. Select the **Enable Trace Logging** check box.
- e. Select the tracing options you need.
- f. Now activate the program, process, or report that is causing the performance issue.

The client (UI Trace) log generates, using your selected options.

Run these logs for as long as you need; when they have gathered enough information, you can then deactivate them.

## Generate Server Logs

You next generate one or multiple application server (appserver) logs to send to Epicor Technical Support. These logs are key for resolving your issue, as they help the support team see what is occurring in your system.

You first activate server logs in the Epicor Administration Console. Then repeat the activity in the Epicor ERP application that caused the issue. If you are tracking a performance issue, you may need to generate multiple server logs to record during what time periods your organization experiences slow performance.

 **Tip** To learn more about evaluating performance issues and the tools you can use, review the Performance Tuning Guide. This guide is available in the application help in the System Management > Working With System Management node.

1. Log into your server machine.
2. Launch the **Epicor Administration Console**. If this program is not on the desktop, launch a search to find it. You can also launch it by clicking **Start > All Programs > Epicor Software > Epicor(VersionNumber) > Epicor Administrative Tools > Epicor Administration Console**.
3. Expand the **Server Management** node and the **[ServerName]** node.
4. Select the application server that runs your Epicor ERP application.
5. Launch the **Application Server Settings** window. You can do this in the following ways:
  - a. Right-click the **[ApplicationServer]** node; from the context menu, select **Application Server Settings**.
  - b. From the **Actions** pane, select **Application Server Settings**.
  - c. Click the **Action** menu; select **Application Server Settings**.
- The Application Server Settings window displays.
6. Select the **Trace Log Enabled** check box.
7. Now for the **Max Log File Size** field, enter how large each file size can grow until the Epicor Administration Console creates a new server log file.

Notice you can limit the file size using **Bytes**, **Kilobytes**, **Megabytes**, and **Gigabytes**.

**8.** Next select the following **Standard Logging** options:

- a. **Verbose Logging** -- Causes the server log to display all the details for each method call sent to the server.
- b. **Trigger Hits** -- Records additional information about trigger activity that occurred.
- c. **BPM Logging** -- Tracks any Business Process Management (BPM) directives currently running on your system.
- d. **Detailed Exceptions** -- Displays information about any exception messages that displayed while the server log ran.
- e. **ERP DB Hits** -- Adds information about database activity to the server log. This activity originates from the Epicor ERP application.
- f. **BAQ Logging** -- Tracks any Business Activity Query (BAQ) transactions that ran against your Epicor ERP database.

**9.** If you evaluating a performance issue, select these **Advanced Logging** options:

- a. **System DB Hits** -- Adds information about database activity to the server log. This activity originates from the server.
- b. **System Table Methods** -- Details any methods that the system ran.



**Important** If you are not reporting a performance issue, do not select these Advanced Logging options. These options will slow system performance.

**10.** Click **Apply**.

**11.** Click **OK**.

This message displays: WARNING: Changes made to these settings will cause the current Epicor ERP instance to restart. Do you want to save the changes?

**12.** Click **Yes**.

**13.** Now within the Epicor ERP application, either repeat the steps that caused the issue or run the daily routine over a series of working days.

**14.** When you are satisfied that the server log(s) contains enough information about the issue, use **Windows® Explorer** to navigate to the **c:\inetpub\wwwroot\EpicorTest10\server** directory.

**15.** Copy all the **ServerLog** files to the **EpicorSupport** directory.

**16.** Compress these files using **7zip**, **WinRAR**, or the built in Windows zip utility.



**Tip** Epicor Technical Support recommends you always generate server logs. The Standard Logging options do not affect performance, so by continuously generating server logs you will already have a series of logs to send to support. However if you generate server logs using the Advanced Logging options, be sure to shut them off after Epicor Technical Support has received enough data.

## Capture Logs

You next capture application server logs and database server logs by first indicating which types of logs you want to save to the Results Path location(s). You then run the capture process.

This process creates a backup copy of each application server log and/or database server log. The original logs are still available in the server directory location.

1. Launch the **Performance and Diagnostic Tool**.
2. From the **Plugins** tree view, select the **Log Capture** node.  
The **Server Information > App Servers** sheet displays.
3. Select the application servers you need to trace.
4. Click on the **Servers Information > DB Server** sheet.
5. Select the database servers you need to trace.
6. Click on the **Logs Capture** sheet.
7. Select the **Backup All Servers Logs** check box to cause the Performance and Diagnostic Tool to copy all server logs to the Results Path location(s).
8. If you want to include event logs as well, select the **Backup All Event Logs** check box.
9. To add the web.config and machine.config (configuration) files to the Results Path location(s), select the **Backup webconfig and machine config** files check box.
10. Click the **Run Log Capture** button.

The **Log** field details the capture process and indicates when this process is complete. The Performance and Diagnostic Tool selects logs from the application servers and the database server directory folders and then copies them to the Results Path location or locations. You can then access these log files from the designated folder or folders.

## Send the Data

After you have gathered the files and logs described in the previous topics, you are ready to send the data to Epicor Technical Support and start your support call.

1. Navigate to the **EpicorSupport** folder that contains the files you generated and gathered.
2. Compress these files contained in this folder. Use **7zip**, **WinRAR**, or the built in Windows zip utility.
3. If you have a call number for this issue, name the file **[CallNumber].zip** or **[CallNumber].rar**. If you do not have a call number, use your Site ID and name the file **[SiteID].zip** or **[SiteID].rar**.
4. Now send this file to Epicor Technical Support.
  - a. If the compressed file is less than 5MB in size, send the file as an email attachment.
  - b. If the compressed file is larger than 5MB in size, upload the compressed file to the **Epicor Support FTP** site. The rest of the steps in this topic describe how you upload the file to this site.

5. Using your internet browser, navigate to **ftp://ftppmpls.epicor.com/**.
6. Log into the FTP site. Enter the **User name** and **Password** you use to log into **EpicWeb**.
7. Copy your compressed file.
8. Paste this file on the **Incoming** folder icon.



**Important** Do not open the Incoming folder. You only need to paste the .zip file onto the Incoming folder icon.

The file upload process runs.

9. When this process is complete, send Epicor Technical Support an email that details your issue and include the name and the size of the uploaded file.
10. Epicor Technical Support will review your information and contact you as soon as possible.

## Performance and Diagnostic Tool

---

Use the Performance and Diagnostic Tool to evaluate how the Epicor application performs through client, server, and network tests. You also use this tool to evaluate the system configuration and download additional diagnostic resources for use with SQL Profiler.

If you are experiencing performance issues, you should first contact either your Epicor consultant or Epicor Technical Support. If the performance issue cannot be resolved through this initial contact, the technical support representative or the consultant may recommend you use the Performance and Diagnostic Tool. This tool captures performance information, and you can organize this information to receive meaningful metrics that relate to the performance of your Epicor ERP application. You can also export these results to Microsoft® Excel® for additional review and analysis.

Through the Performance and Diagnostic Tool, you can evaluate:

- The performance of one client versus another client on the same system.
- The performance of business object methods on both the client and the server.
- Overall performance of the server and the network.
- Performance of business objects in one system against the same business objects on other systems.
- Performance of customizations, personalizations, Business Process Management (BPM) methods, and business activity querys (BAQs).
- The configuration of the Epicor ERP application.



**Important** The Performance and Diagnostic Tool released with Epicor ERP version 10 is only compatible with the 10.0.600 version or higher. If you need to evaluate the performance of Epicor ERP 9.05 or earlier, download the Performance and Diagnostic Tool released with the 9.05 version.

To learn more about the Performance and Diagnostic Tool, review the **Performance Tuning Guide**. This guide describes the common patterns of slow performance, the tools available for testing performance issues, and potential performance solutions. This guide is located in the application help in the **System Management > Working with System Management > Performance Tuning Guide** node. You can also access this guide from the Performance and Diagnostic Tool; to do this, click the **Help** menu.

## Verify SSL Certificate Friendly Name

---

The SSL certificate you use for Epicor Server must have a Friendly Name assigned so that the server could recognize it. Use these steps to check the certificate you want to pick has a Friendly Name.

**1. Launch Microsoft Management Console.**

- If you are on Windows Server 2008 R2, click **Start**. Click in the **Start Search** text box, type **mmc**, and then press **ENTER**.
- If you are on Windows Server 2012, press the **<Windows> + F** button to display the Charms bar. Select **Apps** and in the search box, enter **mmc**.

**2. Click File > Add/Remove Snap in...**

**3. From the list of Available snap-ins, select Certificates and click Add.**

**4. In the Certificates snap-in window, select the option to manage certificates for Computer account. Click Next.**

**5. In the Select Computer window, select the option to manage certificates for Local computer. Click Finish.**

**6. Expand the Certificates (Local Computer) node.**

**7. Browse to the Personal > Certificates folder.**

**8. Right-click the certificate you want to assign to Epicor Server and select Properties.**

**9. Verify the Friendly Name field has a value entered or enter a name for the certificate if it is missing.**

**10. Click OK.**

# Index

.sysconfig file 176, 177, 178, 187, 193, 195, 196, 197

## A

abandoned errors 266  
account lockout policy 123  
account lockout policy, windows 127  
account lockouts 123  
account, administration 42, 43, 44  
account, database manager 45  
accounts, unlock 125  
active licenses 84  
active users 84  
active users, licenses 84  
administration account 42, 43, 44  
administration console, regenerate data model 88  
advanced financial reporting 239  
afr database, restore 239  
afr replication tasks, delete 239  
afr replication tasks, recreate 241, 242, 243  
application cache 206, 207  
application data, gather 348  
application help, ewa 216  
application security 166  
application server information, gather 346  
application server, create 46  
application servers, prerequisites 46  
application settings 178  
architecture, epicor erp 16, 18, 19  
asp.net impersonation 324  
attachments 277  
audit logs 279  
authentication security 119  
authentication, windows account 127  
authorization security 161  
auto job closing log 256  
auto job completion log 257  
auto job firm log 257  
auto job release log 258  
automatic schedules 200, 201, 202, 203, 204  
automatic sign on 126

## B

backup database, manual 96  
backup maintenance plan 97, 98, 99  
backup, differential 101  
backup, full 100  
backup, restore 103, 240  
backup, transaction log 101  
bank statement conversion log 248  
basichttbinding 28  
binding options 31  
bindings 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39  
bindings, custom 40  
bpm directives, disable 341

bpm directives, recompile 342  
bulk address validation log 248

## C

calculate global scheduling order log 259  
call logs 279  
can preview, cannot print 330  
cannot find report 331  
cannot generate sspli context error 319  
cannot log into modern shell 325  
cannot print to a client printer 332  
capture logs 351  
change log 281  
change log report 174  
clear application cache 206, 207  
clear cache, ewa 212  
client logs, generate 348  
client trace log 292, 300, 302, 303  
client trace log, activate from client 297  
client trace log, user account 295  
command line, regenerate data model 90  
company security 162  
component flow 20  
compression 29  
configeditor tool 176, 177  
configuration file, regenerate data model 90  
configuration files 347  
configuration settings file 176, 177, 178, 187, 193, 195, 196, 197  
configuration settings file, alternate 197  
connectivity errors 318, 319  
conversion log 303  
conversion workbench 207  
convert pcinvalues log 260  
create database permission denied 320  
create table permission error 333  
crm license, ewa 219  
crm license, mes 219  
crystal reports, ewa 214  
custom bindings 40  
customization/personalization maintenance 208  
customizations, check 341  
customizations, ewa 217

## D

dashboard maintenance 208  
dashboards, ewa 218  
data fix workbench 209  
data health check workbench 209  
data model customization 94  
data model customization, exclude schemas 95  
data model customization, excluded tables 94  
data model customization, include schemas 94  
data model customization, included tables 94

data model customization, table standards 94  
 data model generator file 89  
 data tag maintenance 209  
 database error, create database permission denied 320  
 database error, index outside bound of array 321  
 database error, server data directory 322  
 database error, size too small 320  
 database errors 320  
 database manager account 45  
 database migration 245  
 database migration log 303  
 database, move 231, 233, 234  
 database, purge 104  
 database, restore 103  
 delete afr replication tasks 239  
 demand entry logs 285  
 demand header log 285  
 demand line log 290  
 demand schedule log 290  
 deployment settings 193  
 desktop icon, regenerate data model 91  
 detect redundant boms log 260  
 diagram, component flow 20  
 diagram, report/process flow 23  
 differential backup 101  
 distribution logs 256

**E**

ecc convert web customer part uom log 273  
 ecc customer consumer synchronization log 253  
 ecc supplier synchronization log 254  
 email notification 103  
 embedded education, ewa 214  
 enterprise configurator direct log 271  
 enterprise configurator log 270  
 enterprise search, ewa 215  
 environments, multiple 220  
 epicor account authentication 120  
 epicor erp architecture 16, 18, 19  
 epicor erp, manage 119  
 epicor support checklist 339  
 epicor web access 212  
 error message log 304  
 error message logs 343  
 event viewer 313  
 event viewer files, gather 348  
 ewa deploy, web application folder error 322  
 ewa errors 322  
 ewa license options 219  
 ewa, clear cache 212  
 ewa, configure help 216  
 ewa, crm license 219  
 ewa, crystal reports 214  
 ewa, deploy customization error 323  
 ewa, deploy customizations 217  
 ewa, deploy dashboards 218  
 ewa, embedded education 214  
 ewa, enterprise search 215  
 ewa, invalid user id 324  
 ewa, manage 212  
 ewa, mes license 219

ewa, time and expense license 219  
 exclude schemas 95  
 expire passwords 121  
 export report 235  
 export to mattac log 254  
 extensions 58

**F**

field security 172, 173  
 file attachment maintenance 210  
 financial logs 248  
 fix banktran reporting amounts log 249  
 fix book detail records log 274  
 fix book release records log 274  
 full backup 100

**G**

generate purchase schedules log 284  
 generate purchasing suggestions log 283  
 generic import log 255  
 generic integration log 255  
 global scheduling log 261  
 global security manager 163

**H**

help settings 195  
 how its organized 14  
 http 28  
 httpbinaryusernamesslchannel 34  
 https 28  
 httpsbinaryusernamechannel 35  
 httpsbinarywindowschannel 36  
 httpoffloadbinaryusernamechannel 37

**I**

impersonation 324  
 import edit demand log 290  
 import labor scheduling parameters log 261  
 include schemas 94  
 index outside bound of array 321  
 indexes, rebuild 85, 86, 87  
 insufficient winsock resources 319  
 integration logs 253  
 intended audience 14  
 interface security 161  
 invalid user id, ewa 324  
 issue details 344

**L**

layer verification failure 325  
 license options, ewa 219  
 licenses, activate 81  
 licenses, active 84  
 load balancer connectivity 318  
 load level 264  
 lob data exceeds maximum 333

locked accounts 124  
locked accounts, track 124  
locked accounts, unlock account level 125  
locked accounts, unlock server level 125  
log, auto job closing 256  
log, auto job completion 257  
log, auto job firm 257  
log, auto job release 258  
log, bank statement conversion 248  
log, bulk address validation 248  
log, calculate global scheduling order 259  
log, change 281  
log, conversion 303  
log, convert pcinvvalues 260  
log, database migration 303  
log, demand header 285  
log, demand line 290  
log, demand schedule 290  
log, detect redundant boms 260  
log, ecc convert web customer part uom 273  
log, ecc customer consumer synchronization 253  
log, ecc supplier synchronization 254  
log, enterprise configurator 270  
log, enterprise configurator direct 271  
log, error message 304  
log, export to mattec 254  
log, fix banktran reporting amounts 249  
log, fix book detail records 274  
log, fix book release records 274  
log, fix recalculate customer credit 250  
log, generate purchase schedules 284  
log, generate purchasing suggestions 283  
log, generic import 255  
log, generic integration 255  
log, global scheduling 261  
log, import edit demand 290  
log, import labor scheduling parameters 261  
log, manufacturing lead time calculation 262  
log, material requirements planning 262  
log, mrp 262  
log, multi-company 272  
log, multi-company direct 272  
log, planning workbench job 267  
log, plm 256  
log, posting engine 249  
log, process mrp recalculation needed 268  
log, production yield recalculation 268  
log, recalculate bank balances 250  
log, refresh order release quantity 274  
log, refresh partbin qoh from parttran 269  
log, regenerate configurations 291  
log, release data locked for gl posting 251  
log, remove orphaned pickedorders mtlqueue 275  
log, rohs job compliance 269  
log, rohs part compliance 269  
log, rohs supplier pricelist compliance 285  
log, server 305  
log, system activity 175, 309  
log, task agent 311  
log, transaction 283  
log, transfer balances 251  
log, ud codes creation for intrastat 251

log, unlock bank statement 252  
log, unlock batch 252  
log, use tax calculation 252  
log, verify balance records 253  
log, verify existing configurations 291  
logging 248  
logging level 264  
login, layer verification failure 325  
login, maximum users 326  
login, server rejects client credentials 329  
logon error, impersonation 324  
logon errors 324  
logon fails for execution account 334  
logon failure audit report 174  
logon, modern shell issue 325  
logon, no license configured for company 327  
logon, open exception error 328  
logs, audit 279  
logs, call 279  
logs, capture 351  
logs, demand entry 285  
logs, distribution 256  
logs, financial 248  
logs, integration 253  
logs, manufacturing 256  
logs, multi-company 270  
logs, multi-tenant 273  
logs, program 275  
logs, purchasing 283  
logs, sales 285  
logs, system 292

## M

main details, gather 343  
maintenance plan, backup 97, 98, 99  
maintenance plan, email 103  
maintenance plan, finish 102  
manage epicor erp 119  
management programs 207  
manual backup 96  
manufacturing lead time calculation log 262  
manufacturing logs 256  
material requirements planning log 262  
maximum users exceeded 326  
memos 275  
menu control, run time argument 166  
menu security 167, 168, 169  
menu security report 174  
metadata output path error 322, 323  
method changes 246  
method security 170, 171  
model, n-tier 16  
model, three-tier 16  
model, two-tier 16  
move database 231, 233, 234  
move report 235, 236, 237, 238  
mrp log 262  
multi-company log 272  
multi-company logs 270  
multi-tenant logs 273  
multiple environments 220

multiple sites, ssl certificates 39

## N

net.tcp 28  
 network protocols 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39, 40  
 no error 337  
 no license configured for company 327  
 non scheduling time 267  
 number of mrp processors 267  
 number of schedulers 267

## O

open exception error 328

## P

password management 122  
 password policy 120, 121, 122  
 password policy, windows 127  
 pending status, all reports have 329  
 performance and diagnostic tool 352  
 permissions granted error 335  
 personalization purge 210  
 pid 263  
 planning workbench job log 267  
 plm log 256  
 posting engine log 249  
 potential sources, eliminate 340  
 print outages 329, 330, 331, 332, 333, 334, 335, 336, 337, 338  
 print process times out 336  
 printer setting 336  
 printer 336  
 no printing. error 336  
 process control customizations 264  
 process flow 23  
 process mrp recalculation needed log 268  
 process sets 201, 203, 204  
 processor identifier 263  
 processor log 263  
 production db to test db 231, 233, 234  
 production yield recalculation log 268  
 program logs 275  
 programs, identify 343  
 protocol selection 30  
 pull max 267  
 purchasing logs 283  
 purge database 104  
 purge tasks 106  
 purpose of this guide 14

## Q

query conversion maintenance 210

## R

rebuild indexes 85, 86, 87  
 recalculate bank balances log 250

recalculate customer credit log 250  
 record steps to duplicate 345  
 recreate afr replication tasks 241, 242, 243  
 recurring task, regenerate data model 92  
 refresh order release quantity log 274  
 refresh partbin qoh from parttran log 269  
 regenerate configurations log 291  
 regenerate data model 87, 88, 89, 90, 91, 92, 94, 95  
 release 245  
 release data locked for gl posting log 251  
 release updates 245  
 remote machines, configure 74  
 remote name does not resolve 337  
 remove orphaned pickedorders mtlqueue log 275  
 report flow 23  
 report style maintenance 235, 236  
 report, change log 174  
 report, export 235  
 report, logon failure audit 174  
 report, menu security 174  
 report, move 235, 236, 237, 238  
 report, user session 175  
 report, users/groups 175  
 restore afr database 239  
 restore backup 103, 240  
 restore database 103  
 reverse proxy connectivity 318  
 rohs job compliance log 269  
 rohs part compliance log 269  
 rohs supplier pricelist log 285  
 run time arguments 166, 167, 197, 198

## S

sales logs 285  
 scheduler log 265  
 schedules, automatic 200, 201, 202, 203, 204  
 schema changes 246  
 security authentication 119  
 security group conflicts 169  
 security group maintenance 162  
 security groups, assign 165  
 security logic hierarchy 165  
 security management 173  
 security manager 163  
 security manager, global 163  
 security privileges 162  
 security, assign 166  
 security, company 162  
 security, field 172, 173  
 security, interface 161  
 security, menu 167, 168, 169  
 security, method 171  
 security, service 170  
 security, service and method 170  
 security, user 163  
 security, user account 163  
 self-signed certificates 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230  
 send data to support 351  
 serialization 29  
 server data directory 322

server log 305  
server logs, generate 349  
server printing fails 337  
server rejects client credentials 329  
server security 42  
service security 170  
settings list, .sysconfig 178  
setup configuration data 347  
sever file download 316  
single sign on 128, 129, 130, 131  
solution workbench 237, 238  
sort settings 196  
special characters list 122  
ssl certificates, multiple sites 39  
sspi context error 319  
ssrs style does not display 338  
standalone options, regenerate data model 89  
steps to duplicate 345  
support checklist 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 351  
support, send data 351  
system activity log 175, 309  
system activity log purge 211  
system data, gather 346  
system information, gather 346  
system logs 292  
system monitor 205  
system tasks 42

## T

table standards 94  
task agent data 347  
task agent log 311  
task agents, add 74  
tasks, purge 106  
tasks, system 42  
tier model 16  
time and expense license, ewa 219  
total non scheduling time 266  
total wait/scheduling time 267  
trace log, activate from client 297  
trace log, activate from user account 295  
trace log, client 292, 300, 302, 303

transaction log 283  
transaction log backup 101  
transfer balances log 251  
transport encryption methods 29  
troubleshooting 318

## U

ud codes creation for intrastat log 251  
unfirm jobs, scheduling 265  
unlock accounts 125  
unlock bank statement log 252  
unlock batch log 252  
updatable query maintenance 211  
updates 245, 246  
use tax calculation log 252  
user account, password options 122  
user accounts 163  
user authentication 29  
user identity security 119  
user interface changes 247  
user security 163  
user session report 175  
user settings 187  
usernamesslchannel 33  
usernamewindowschannel 31  
users, active 84  
users/groups report 175

## V

verify balance records log 253  
verify existing configurations log 291

## W

wait/scheduling times 265  
webhttpbinding 29  
windows 32  
windows account authentication 127  
winsock resources, insufficient 319  
wshttpbinding 29



Additional information is available at the Education and Documentation areas of the EPICweb Customer Portal. To access this site, you need a Site ID and an EPICweb account. To create an account, go to <http://support.epicor.com>.