Epicor ERP
System Administration Guide
10.1

Disclaimer

DOC0091E9

10.1

Revision: December 01, 2015 5:50 p.m.

Total pages: 243

sys.ditaval

Contents

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.

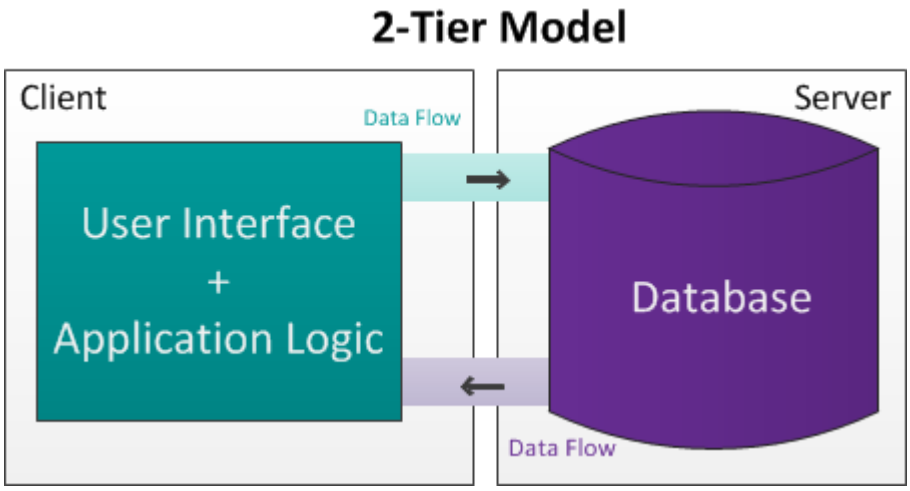
By understanding how the Epicor ERP application is designed, you can better interpret the system messages the application sends you and more quickly resolve issues.

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.



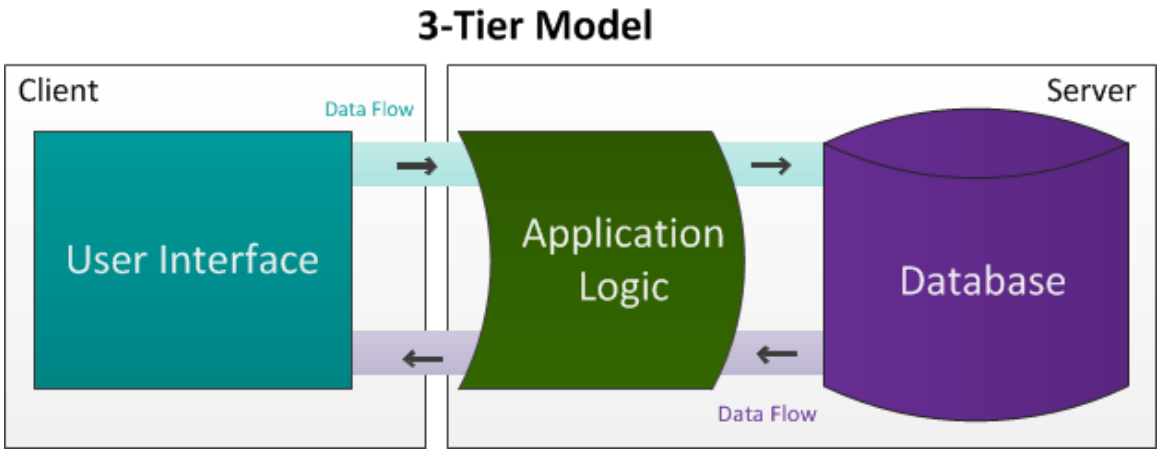
The major disadvantage to this model is all updates must be run individually on each client machine. Any issues that occur must also be resolved individually on each client machine, making both installation and update tasks a cumbersome process.

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

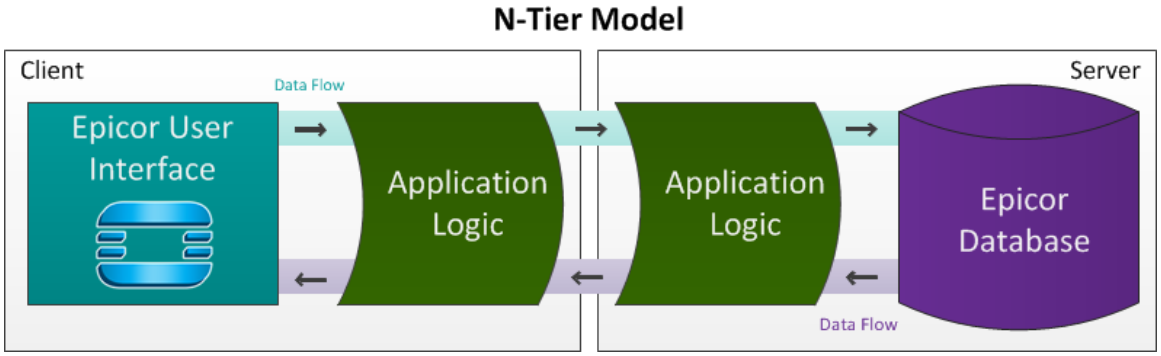
3. Database



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.

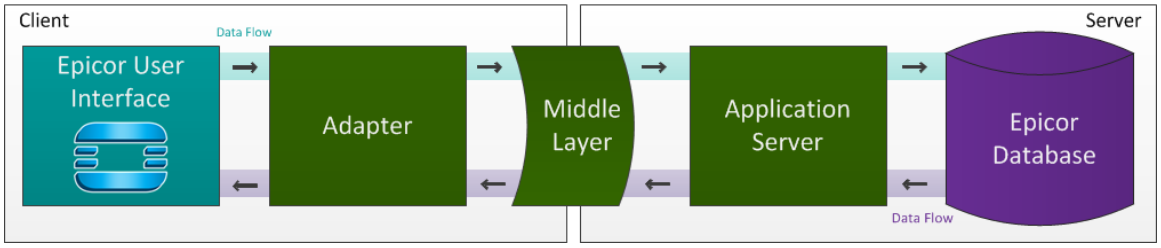


Although this model does not capitalize on the use of shared memory and introduces an additional network connection you do not have in the logical three-tier model, the deployment flexibility of this model has significant benefits for managing enterprise processes.

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.

Architecture Layers



Information about each architecture level:

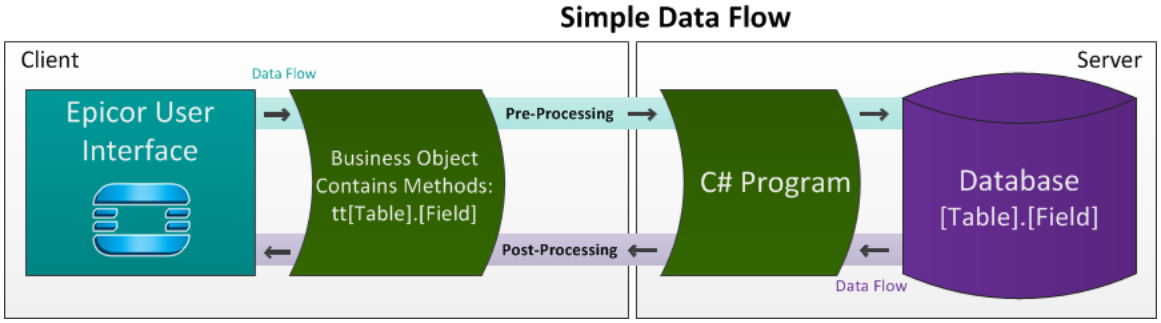
- **User Interface (UI)** - The user interface layer contains the program windows that display for the end user.
- **Adapter** - The adapter typically defines how the business object manipulates the data both before and after a call. The adapter file is placed in the client directory. It processes the transaction between the user interface and the business object that runs a specific process 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.

Simple Data Flow



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,

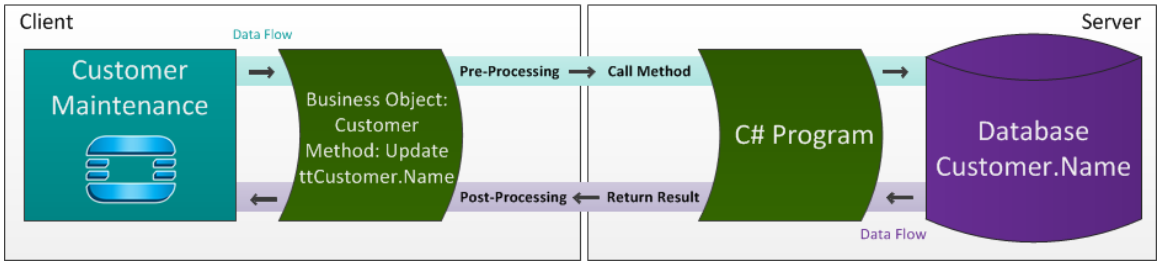
Update, Delete, and other methods that run the changes users make to the Customer table. Notice these methods initially store data in active memory through a series of temporary tables (tt) tables that mirror both the table name and the field name which store the data in the physical database.

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.

Example Data Flow

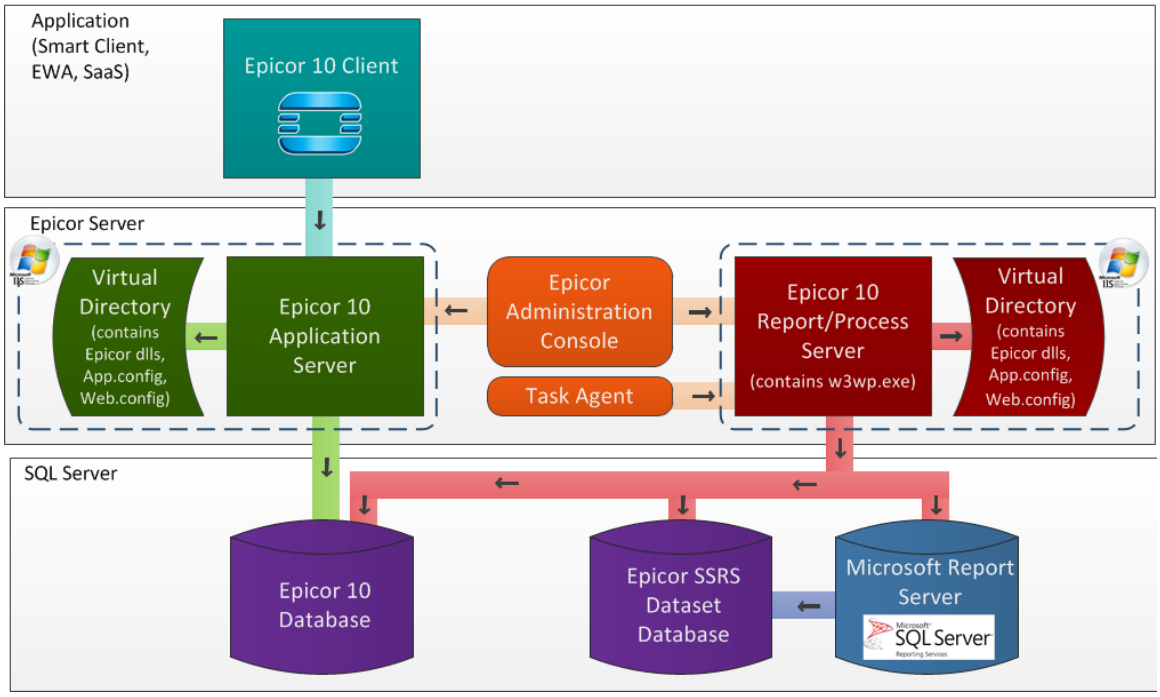


Notice the Update Customer method connects with the C# Code on the server layer. The updated customer record is saved to the physical database, and the resulting data returns for display on the user interface.

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 send 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 the 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.

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** 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, Social Enterprise, and 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. Click the **Ping Server** button to verify the server name.

7. A message displays that the connection is successful. Click **OK**.

8. 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\Epicor10.1.300.

   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 **Net TCP Binding Configuration** drop-down list. When a user logs into the application, the selected method checks whether the user can access the Epicor application.

   Available options:

   - **UsernameWindowsChannel** - Authenticate using an Epicor Username and Password. Only use this method for application servers that run the Epicor Web Access (EWA) and mobile access client installations; Windows checks for existing Epicor user accounts to authenticate logins.
   - **UsernameSSLChannel** - Authenticate using a Secure Sockets Layer (SSL) X509 certificate. 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.
   - **Windows** - Authenticate using a Windows Username and Password. 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.

   Tip For information on how you set up each authentication method, review the **Epicor 10 Architecture Guide**.

6. When you select the UsernameSslChannel for the Net TCP Binding Configuration, 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 Net TCP Binding Configuration, 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. 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.

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. By default the **Application Pool Name** uses the value you entered in the **Application Name** field. You cannot change this value. This value defines the name of the application pool associated with the new application server.

    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.

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 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.

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. 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.

5. 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" />`.

6. 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.

7. Now within the **Epicor Application Launcher** section, select one of the following options:

   a. **Do not allow access to user details** - No method is used to launch the Epicor client. The default value, the client is launched as normal.

   b. **Use Epicor Smart Client** - If you select Use Epicor Smart Client, you need to click the **Browse** (...) button to find and select the **Epicor.exe** file you will use to launch the Epicor client.

   c. **Use Epicor Web Access** - If you use Epicor Web Access, 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 Epicor Web Access (set within the client).

8. 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.

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.

   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. If you are updating the application server and you do not need to deploy the SSRS reports, be sure to clear the Import Reports check box.

   Important While you can clear the Import Reports check box, do not clear the Configure SSRS check box. If you clear this check box, it indicates you no longer use SSRS reporting, causing the application server to reconfigure without the SSRS functions.

10. For the **SSRS ReportServer Location**, select the directory that contains the SSRS **ReportServer** installation. Depending on the SQL Server version you use, this location is similar to the following example directories.

Your specific directory path will be the name your system administrator assigned to the SQL Server instance during installation.

- **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. Typically this directory is: \\<RemotePCName>\C$\Program Files\Microsoft SQL Server\MSRS10_50.MSSQLSERVER\Reporting Services\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**.
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.

   Important One error you may receive is that 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.

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.

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, Social Enterprise, and Epicor Education (Embedded Courses).

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**, **Social Enterprise**, **Epicor Education**, and **Information Worker** 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. Next enter the **Virtual Directory** name for the Epicor Web Access extension. The default directory is EpicorWebAccess. You can change this value to any name that Internet Information Services (IIS) will accept. The Epicor Web Access files are then saved in the directory you enter in this field.

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 Blackberry, iPhone, 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 **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. Next enter the **Virtual Directory** name for the Epicor Mobile Access extension. The default directory is EpicorMobileAccess. You can change this value to any name that Internet Information Services (IIS) will accept. If you use the default value, a virtual directory is created in IIS using a physical path and folder located under the \inetpub\wwwroot folder.

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.

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.

   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 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 the **Server Name** for the database server that contains the database you will use with this Enterprise Search database.

3. 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.

4. 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.

5. 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.

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

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

8. 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.

   e. **Extension URL** - Displays the internet website for the Enterprise Search extension. You can click this link to launch your internet browser and display the website.

9. 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.

10. 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.

Social Enterprise

Epicor Social Enterprise is an information network designed to support information exchange across your business enterprise.

Epicor Social Enterprise is fully integrated into the Epicor ERP application's smart and web clients. From each client, you can access the Epicor Social Enterprise website and work with the full functionality of your Epicor Social Enterprise account, or you can choose to work in Epicor Social Enterprise in the context of a selected ERP data record.

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

1. You use this sheet to install a new Social Enterprise extension or add an existing extension. You can also update the current Social Enterprise extension.

   a. To install a new Social Enterprise extension, click the **New** button. Enter the **Deployment Name** for this extension. Be sure to enter a name that helps you identify each Social Enterprise extension available on your system.
   The fields on the Social Enterprise sheet activate for data entry.

   b. To add an existing Social Enterprise extension, click the **Browse** (...) button.
   The Application Server Settings program locates existing Social Enterprise extensions; select the extension you wish to add or update. After you select the Social Enterprise extension, the fields activate for data entry.

   c. To update the Social Enterprise extension, enter the new values in the fields on this sheet.

2. Enter your name for the Social Enterprise site in the **Web Site** field. If you do not have a name you wish to us, accept the **Default Web Site** value.

3. Enter the **Server Name** for the database server that contains the database you will use with the Social Enterprise database. you can find this value by navigating to the **Application Server > Database Connection** sheet.

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 for the **Database Name**, enter name of the SQL database linked to the current application server. To find this name, navigate to the **Application Server > Database Connection** sheet.

6. If you are setting up Social Enterprise for the first time, select the **Create DB** check box. When you select this option and click **OK**, a new database is generated using the name you entered in the **Server Name** field. If you update the Social Enterprise 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 Social Enterprise database, you cannot create a new database. If you wish to create a new Social Enterprise 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 > Social Enterprise 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 database, click **Test Connection** and click **OK** in the confirmation message.

8. If you are installing Epicor Social for the first time, use the **Initial Account** fields to create the initial user of the Social Enterprise system. Enter your **User Name** and **Password** which will be used to login to Social Enterprise.

   The password must be eight or more characters. It is recommended that you keep a record of the data you enter in this field, as you will need to reference it later.

9. You next specify the user account used to connect Social Enterprise with the **CDC Service**. Use the following fields:

   a. **Built In Account** - Enter the default account created for the CDC Service.

   b. **User** - Enter the User ID for a custom account you wish to use.

   c. **Password** - Enter the password for the custom account.

   Important If your Epicor ERP application server uses Windows authentication, you must enter a custom account for the Epicor Social Enterprise extension. The custom account you use is same account that you specified within the CDC service.

10. The **Current Deployment** section details the state of the Social Enterprise 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 Social Enterprise 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 Social Enterprise extension.

    e. **Extension URL** - Displays the internet website for the Social Enterprise 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.

11. When you finish updating the Social Enterprise 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 Social Enterprise extension is now added to your Epicor ERP environment.

Important After you deploy the Social Enterprise 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 us, accept the Default Web Site value.

5. Next enter the **Virtual Directory** name for the Epicor Education extension. The default directory is EpicorEducation. You can change this value to any name that Internet Information Services (IIS) will accept. If you use the default value, a virtual directory is created in IIS using a physical path and folder located under the \inetpub\wwwroot folder.

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. Enter the **Epicor User Name** and **Password** to use for the connection to application server. The course web site uses this User ID and Password to login to the Education Application Server to verify licensing information. The default User ID and Password for the Epicor Education database is epicor/epicor.

9. For the **Operation timeout**, define how long you want an inactive operation to continue processing until it is stopped by the application server.

10. If you selected UsernameSSLChannel authentication type for this Epicor Education extension, you must also select the **Validate WCF Certificate** check box.
This causes the system to check whether the WCF Certificate is current.

11. 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.

12. 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.

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

14. Launch the **Epicor ERP** application.

15. Navigate to **Company Maintenance**.

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

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

17. 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 us, accept the Default Web Site value.

5. Next enter the **Virtual Directory** name for the Information Worker extension. The default directory is InfoWorker. You can change this value to any name that Internet Information Services (IIS) will accept. If you use the default value, a virtual directory is created in IIS using a physical path and folder located under the \inetpub\wwwroot folder.

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.

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

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. Users create these schedules in the Epicor ERP application using **System Agent Maintenance**.

You can set up a maximum of three task agents to run against the same application server. By setting up multiple task agents, you ensure the Epicor ERP application continues to process tasks when a task agent fails. If a process doesn't 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.

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

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 3.0.4.0 and Task Agent Service Configuration for 3.0.5.0 installed on the same machine. Through this feature, you can have multiple versions of the service running at the same time. In the control panel, each instance of the service displays as a separate icon identified by its version number.

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.

When you use the firewall in Windows 7, do the following to activate remote access:

1. Depending on your server, you locate the Windows Firewall in different ways:

   a. For **Windows Server 2008**, click **Start**. In the **Search** field, enter **Windows Firewall**. Select Windows Firewall from the search results.

   b. For **Windows Server 2012**, press **<Windows> + F** on your keyboard to launch the **Search** bar. Click on the **Apps** button. Find and select the **Windows Firewall with Advanced Security** icon.

   The Windows Firewall with Advanced Settings displays.

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.

   Available options:

   - **UsernameWindowsChannel** -- Select this option to authenticate using an Epicor Username and Password. Windows authenticates the user account. You can select this option for both smart client and Epicor Web Access (EWA) installations.
   - **UsernameSSLChannel** -- Use this option to authenticate using a Secure Sockets Layer (SSL) X509 certificate. Use this method for application servers that handle installations where users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor application. If you select this option, you need to define a DNS Endpoint Identity. You can select this option for both smart client and Epicor Web Access (EWA) installations.
   - **Windows** -- Select this option to authenticate using a Windows Username and Password. Windows authenticates using a domain user account. Select this method for application servers that handle client installations where users access the application through the same domain. If you select this option, you do not enter a Username/Password for the task agent on this dialog box; instead you define this domain user account on the Windows service. You can only select this option on smart client installations.

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

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

   Important 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. 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).

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

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, an 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
	**Active** -- 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.
	**Warning** -- 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.
	**Expired** -- 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**.

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_TEMPDBOption, 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) column extensions to existing tables through Extended User Defined Table Maintenance or new tables through the Software Developers Kit (SDK). To complete a database customization, the data model must be regenerated to incorporate the new and/or extended tables.

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.

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.

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

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:\Program Files (x86)\Common Files\Epicor Software Corporation\Database Manager Extensions\<VersionNumber>\DataModelGenerator** directory path.
2. Locate the **Ice.Tool.DataModelGenerator.UI.exe.config** file.
3. Open the 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 Ice.Tool.DataModelGenerator.UI.exe.config file 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:\Program Files (x86)\Common Files\Epicor Software Corporation\Database Manager Extensions\<VersionNumber>\DataModelGenerator** directory path.
2. Locate the **Ice.Tool.DataModelGenerator.UI.exe.config** file.
3. Open the 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.SysAgen
tSchedProcessing</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.

Run the Regeneration

To finish adding the extended user-defined table or SDK created table, regenerate the data model for the Epicor database. Run this task on the server that contains your database. You regenerate the data model through the Epicor Administration Console.

1. On your server machine, press **<Windows> + F** to display the **Search** bar.

2. 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. Expand the **Database Server Management** node and the XXX database server node (where XXX is the name of your database server) that contains the database you need to update.

5. Select the database icon.
   The properties for the database displays in the center pane.

6. From the **Actions** pane, click the **Regenerate Data Model** button.
   The **Generate Data Model** window displays.

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 and close the Epicor Administration Console. Return to the Apps screen and launch the Command Prompt (under the Windows System section). In the Command Prompt window, enter IISRESET and press <Enter>. After IIS stops and restarts, close the Command Prompt window and return to the Epicor Administration Console. You should be able to regenerate the data model.

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 restarting IIS. Restarting IIS is a mandatory task after the data model is successfully regenerated. To do this, launch the **Command Prompt** window.

10. Enter **IISRESET** and press **<Enter>**.

11. After IIS stops and restarts, close the Command Prompt window.

    Tip Using the IISRESET command stops and restarts all the application pools on your system, which can temporarily disrupt some processing. You may be able to regenerate the data model by just stopping and restarting the application pool that runs the Epicor ERP application. You can do this through two programs:

    - **Epicor Administration Console** -- Expand the **Server Management** node and select your application server. From the **Actions** pane, select the **Recycle IIS Application Pool** option.
    - **Internet Information Services (IIS) Manager** -- Select the **Application Pools** node. From the center pane, right-click the application pool for the Epicor ERP application; from the context menu, select the **Recycle** 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, the disk version updates to include the new extended user defined tables and columns.

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.

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.

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 requires 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 uses 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 liked 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. 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. 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.

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. 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

   Important This program is not available in Epicor Web Access.

2. Find and select the user record you need to review.
3. Select the **Expire Password** check box to force the user to enter a new password the next time he or she logs into the application.
4. If you select the **Clear Password** check box instead, the user can enter a blank password when she or he logs into the application. This user is then prompted to enter a new password.
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.

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 accidently 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

   Important This program is not available in Epicor Web Access.

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.

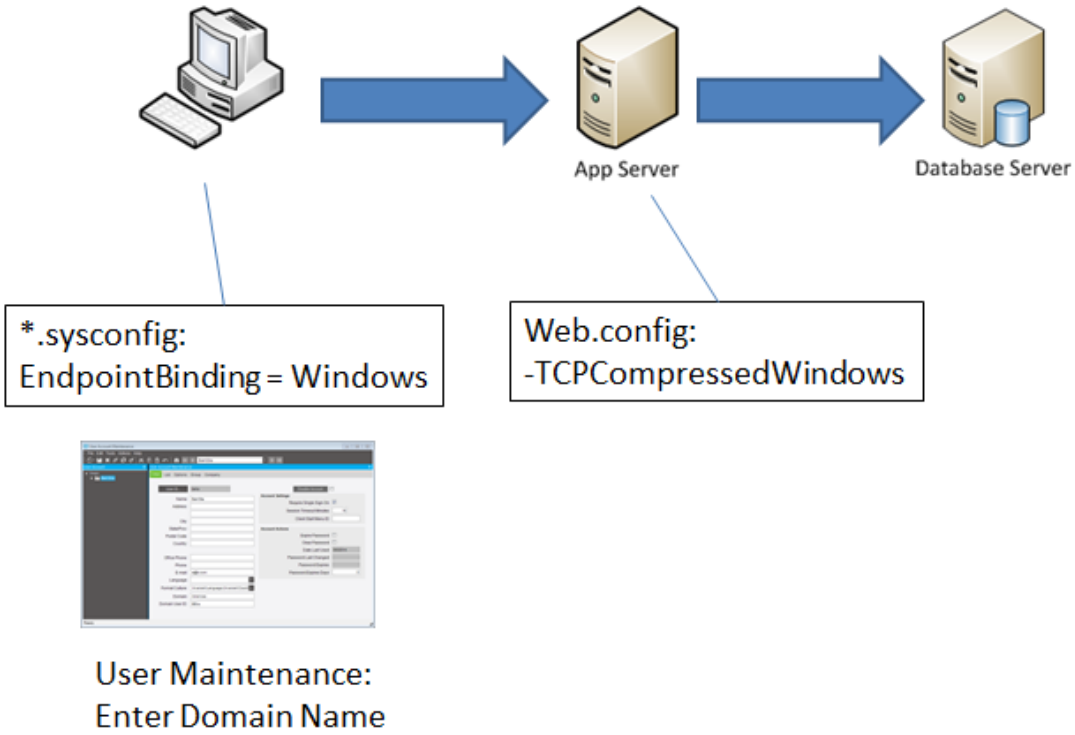
Note For more information on both the password policy and the account lockout policy for Windows accounts, review your Microsoft® Windows® documentation.

Single Sign-On

Single Sign-On (SSO) is a time-saving feature you implement so users can sign on (log in) with the same account they use to log into the Windows operating system. When you enable this feature, users no longer see a Log On window when they click the Epicor ERP application icon; instead the Menu screen displays.

Important This automated login option only work within environments where you control access through the User Name authentication protocols (Windows TCP binding). You cannot use automated login within environments that use token authentication, Windows Channel authentication, or Secure Sockets Layer (SSL) Channel authentication protocols.

To set up the Single Sign-On feature, you must use Windows authentication. You configure the client, server, and application server to authenticate through Windows.



When an application server (AppServer) is configured for Single-Sign On, all connections to that application server must use Single Sign On. If you need some users to log in by entering their User Name/Password, set up a different application server that is not configured for Single-Sign On. These users then log in using this alternate application server.

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

   Important This program is not available in Epicor Web Access.
3. Find and select the user record for which you will activate Single-Sign 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 only access the server through Windows Authentication.
   - The server only runs Windows Authentication 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|Usernameme
WindowsChannel" />
```

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.

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 Process 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 in 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 modify menu and process security options to restrict a module, program, or process to specific users.

Security Manager Rights

The Epicor ERP application restricts access to the System Management 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. So for most installations, you will not use global security manager rights. You assign this status to a group of users within the Epicor Administration Console, or individually through User Account Security Maintenance.

Global security managers have the highest level security available 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

Important This program is not available in Epicor Web Access.

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.

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, 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 your organization uses **Social Enterprise**, enter the **User ID** and **Password** this user needs to access this program. Through Social Enterprise, your users can improve company communication by joining social groups and viewing text streams.

11. 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.

12. 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.

13. 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, process, 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, process, method, or field, this user account cannot use this item.

4. When a specific user account is granted access to a menu, program, process, 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, process, 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, process, 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.

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, Process Security Maintenance, and Field Security Maintenance.

Assign Security

You can assign security to programs, processes, 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.
- **Process Security Maintenance** - Use security groups and user accounts to prevent or allow access to specific business objects (like customers, parts, sales orders, and so on) and/or methods within these business object (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. When you select the **Exclude Epicor Web Access** check box, users assigned to this security code cannot launch the Epicor ERP application through an internet browser.

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.

    Important Be aware when you change the security code for a standard menu item like the AR Invoice Entry, this code reverts back to its original security code when you install the next service pack. You should only use this functionality for custom programs or be prepared to reassign the menu security codes after a service pack installation.

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, Process Security Maintenance, and Field Security Maintenance programs.

Process and Method Security

You launch Process Security Maintenance to establish security at the process level and at the method level within a process.

Use the **Process** sheet to set the security privileges for business objects like Customers, ABC Codes, Tax Regions, and other business objects. Use the **Method** sheet to establish security at the method level within a process. A method is an action that can be taken in a process such as Update, Get New, Approve, and so on.

Example The Terms process (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 business object level (BO.Terms) on this Process 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 business object 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 processes, and from other menu options. Epicor recommends you assign security in a test environment first before you deploy security within your live environment.

Assign Process (Business Object) Security

You define a business object's security 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 process.

1. Navigate to **Process Security Maintenance**.

   Menu Path: System Setup > Security Maintenance > Process Security Maintenance

   Important This program is not available in Epicor Web Access.

2. Click **New**.

3. Click the **Process ID...** button to find and select the process you need.

4. The **Owning Company** field displays the company in which the current process 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 process.
11. Click **Save**.

Assign Method Security

You can also use Process Security Maintenance to define security for methods within a selected business object.

A method is an action which can be run within a process 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 business objects have multiple methods. This sheet is only for more complex business objects that perform a variety of actions.

1. Click **New**.
2. Click the **Process ID...** button to find and select the process 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.

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

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 configiration 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 -- Complete 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.

XML Tag	Purpose and Expected Value
AppServerURL	The address of the application server (AppServer) where the client connects protocol://server:port; it uses the form value " **AppServerDC://servername:port**" • **Protocol:** AppServerDC by default, or else AppServer for load balancing. • **Server:** Host name of the machine that runs AppServer. • **Port:** The port of the broker that runs the application. Default is 9000. Also, AppServer accepts strings and numbers, but the port value accepts only numbers.

XML Tag	Purpose and Expected Value
AlternateCacheFolder	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:\Documents and Settings\All Users\Application Data\Epicor This folder accommodates some environment variables which can be substituted during startup. • **%UserName%:** The Windows ID of the user. (Example: jsmith) • **%UserDomain%:** The Windows user domain. (Example: AMERICAS) • **%AppData%:** The application data folder. (Example: C:\Documents and Settings\jsmith\Application Data) • **%Homepath%:** The home path folder. This location is specified in Local Users and Groups. (Example: C:\Documents and Settings\jsmith • **%AllUsersProfile%:** The location of the All Users profile. (Example: C:\Documents and Settings\All Users)
CultureCode	The ISO language/culture code that defines the specific language and format which displays on the **Logon** window. For example, "sch" (Simplified Chinese). 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.
CustomResourceFile	A path name to a resource file that contains custom images. You can add images to this file by using the **Resource Editor**; 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"
DnsIdentity	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.
DuplicateAttachmentMode	Use this setting to indicate what occurs when two attachments share the same identifier (ID) value. Available options: • **Prompt** - Causes the application to display a window that asks the user to enter a different attachment ID. This is the default option. • **AutoDateStamp** - Causes the application to automatically add the current date to the end of the attachment ID.

XML Tag	Purpose and Expected Value
EnableSslStreamSecurity	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 True.
EndpointBinding	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: • **UsernameWindowsChannel** - Authenticate using an Epicor Username and Password. Windows checks for existing Epicor user accounts to authenticate logins. You can select this option for both smart client and Epicor Web Access (EWA) installations. • **UsernameSSLChannel** - Authenticate using a Secure Sockets Layer (SSL) X509 certificate. Use this method for AppServers that handle installations where users reside in different domains. By using an SSL certificate, users from these different domains can log into the Epicor application. You can select this option for both smart client and Epicor Web Access (EWA) installations. • **Windows** - Authenticate using a Windows Username and Password. You can select this method for AppServers that handle client installations where users access the application through the same domain. Any user who has a Windows Username and Password within this domain can successfully log into the Epicor application. You can only select this option on smart client installations. 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 **Epicor Administration Console**.
EnterpriseSearchURL	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: **1.** User record (User Maintenance) **2.** Company record (Company Configuration) **3.** Configuration Settings File
HelpAboutCopyrightText	The **copyright text** for the About dialog box.

XML Tag	Purpose and Expected Value
HelpAboutCopyrightURL	The **copyright URL** for the About dialog box.
HelpAboutImage	The **bitmap file** for the Help About window
HelpAboutProductText	The product text for the About dialog box.
HelpAboutTitleText	The title text for the About dialog box.
HHCustomMenuID	The menu ID for the sub process that causes customized Handheld menus to load onto your screen. The client's sysconfig file should be set to the MenuID of the form in Menu Maintenance as follows: **<HHCustomMenuID value="HHMN0002" />**
MaxBOMRU	The number of most frequently used business objects whose security settings should be cached when a user logs in. Logic then tracks this number of business objects in the following XML file: `C:\Documents and Settings\All Users\ApplicationData\Epicor\<appserver_and_port>\<version>\<company>\ BOSecMRUList\BOMRUList_<userID>.xml` This cached information helps minimize the number of calls between client and server, improving performance. This is the default location of the cache folder, but it can change based on the AlternateCacheFolder setting .
MaxClssAttrMRU	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. The logic tracks this number of datasets in the following XML file: `C:\Documents and Settings\All Users\ApplicationData\Epicor\<appserver_and_port>\<version>\<company>\ClsAttrMRUListt\ClsAttrMRUList_<userID>.xml` This cached information helps minimize the number of calls between client and server, improving performance. This path is the default location of the cache folder, but it can change based on the AlternateCacheFolder setting .
MESCustomMenuID	The menu ID for the sub process that allows customized MES menus to be loaded.
MESImage	The default image that is used by the MES menu. The default is blank.
OperationTimeOut	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

XML Tag	Purpose and Expected Value
	operation and a callback contract method. The default value is 300 (30 seconds).
PredictiveSearchKeyPressDelay	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).
PredictiveSearchPopupFadeDelay	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).
ProductBrandIcon	An optional icon that appears on the far right of the application Title Bar.
ProductBrandText	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.
ProductLogonImage	An alternate bitmap image that appears in the upper half of the logon dialog box.
ProductID	The product identifier; for example "Epicor".
ResourceFile	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\MfgBaseImages.resources**"
SessionManager	The **Session Manager** tracks all of the instances of the application running on this computer, so that users can launch several instances **without** logging in and consuming an additional license. Typically this will just monitor one user, but it can monitor several instances if **Terminal Services** are enabled. Here are the expected values for this setting: **ActiveHidden** - The default value. This value causes the Session Manager to run, but its icon is not displayed within the **System Tray** . **ActiveInTray** - Causes the Session Manager to run; there is an icon displayed in the Windows system tray. **Disables** - Causes the Session Manager to be turned off. Whenever a shortcut or **Information Worker** 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.
SplashImage	The splash screen image when you first log into Epicor.

XML Tag	Purpose and Expected Value
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 **HH:MM:SS** (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, " **.\res\ToolbarSettings.xml**"
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 "10.0.500".

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	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:
	• **ManualSave** - When used, the **Save Active Form Shortcuts** and **Delete Active Form Shortcuts** options available in the client. Use these options to manually Save and Delete the active forms data.
	  • In the **Classic** mode, these buttons are found on the **Options** menu.
	  • In the **Shell** mode, these buttons are found on the sliding **Context** menu at the bottom.

XML Tag	Purpose and Expected Value
	• **AutoSave** - Open forms and data are automatically saved when the client is closed. • **NeverSave** - No forms data is saved when the client is closed.
AutoScaleMode	The concentration of pixels on the window, to accommodate different geometries of forms in different versions of Windows. • "**None**" - The default. No adjustment of forms is done. • "**Dpi**" - An adjustment (dots per inch) of concentration for pixels is done on forms. The forms are adjusted to adhere to the DPI field on the **Display Properties - Settings - Advanced - General** form in Windows. Common settings are 96 DPI and 120 DPI.
ContextMenuNestingLevel	Use this setting to adjust the size of the context menus. Depending on the value you enter, context menus can become taller or shorter. The expected values are: "**0"** - All **Open With** items display within the **More…** sub-menu. "-**1** " - All **Open With** items are displayed directly on the context menu. "**X** " - 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 **More** … sub-menu. For example: **<ContextMenuNestingLevel value ="0"/>**
DataCollectionUser	Defines whether or not this user is a **data collection user**; these users only have access to Data Collection functionality. Only two values can be used - " **true**" or " **false**"
DefaultSearchFormLocation	This value controls the default location of search forms as they open. Available options: **Top** - 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. **Center** - 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 .
DefaultSearchPageSize	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.

XML Tag	Purpose and Expected Value
FormOpenMode	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. **AutoSearch** - The primary search for each UI form automatically displays as the form launches. **AutoPopulate** - The primary search for each UI form is automatically run, and all selected records automatically populate the form as it displays on your screen.
LastLoginID	This setting is used with the **LoginDefault** setting. When LoginDefault is set to **Last**, the value of LastLoginID is the last user ID entered during the logon process. When LoginDefault is set to **List**, the value of LastLoginID is a series of previously entered user IDs that have accessed the application. For the other LoginDefault setting values, LastLoginID is not used and is typically set to have no value.
LaunchType	Use this setting to switch between the Classic Menu and the Modern Shell Menu. Possible values: "**MainMenu**" - 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. "**Shell**" - Causes the client installation to launch using the Modern Shell Menu. Users navigate the interface through tile groups that contain related programs.
LoginDefault	The login default setting that defines what appears in the **User Name** field. Possible values: "**Last** " - Displays the last user ID that was used. "**List** " - Displays a list of all the recently entered user identifiers. "**Windows** " - Displays the same user ID used to log onto Windows on this client machine. "**None**" - No default value; the User Name field will be blank.
Password	The password used for the automatic login (Epicor Account) feature. This encrypted password is generated by the application when a system administrator activates the **Single Sign On** feature and the current user selects the **Automatically sign on** check box on the **Preferences** window. For more information about how to activate this feature, review the **Single Sign On (Epicor Accounts)** section in the **System Administration Guide**.

XML Tag	Purpose and Expected Value
SelectTextOnEnter	This setting determines whether an entire word or number is selected when you click in a field with a value. Values are true or false. The default is **false**.
SingleSignOn	The choices are **true** or **false (the default)**. A value of **true** 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. 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 **Single Sign On** section later in this guide.
SDKUser	Defines whether or not the user is a Software Developer Kit user, with developer tools available. Only two values can be used - " **true**" or " **false**" 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.
StartSystemMonitor	Defines whether or not the System Monitor will start when the application is launched. Only two values can be used - " **true**" or " **false**"
SmtpServer	The location of the smtp server; the smtp server is required for email.

Style	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.
	
	To use the default Epicor appearance without running the styling features, enter "**None**" in this setting option. If you use this configuration settings file to launch the **Epicor Handheld** 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.
	
	Enter "**Default**" 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.
	
	For example:
	`<Style value="None" options="SpecifyName|None|Default"/>`
	
	`<Style value="Default" options="SpecifyName|None|Default"/>`

XML Tag	Purpose and Expected Value
	<Style value="BlueMain.isl" options="SpecifyName|None|Default"/> <Style value="C:\epicor\MyThemes\BlueMain.isl" options="SpecifyName|None|Default"/>
SystemMonitorNonPriorityPoll	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. This value is measured in milliseconds; the minimum value is 3000.The higher this number can be set, the more network traffic is avoided. This value is used with **SystemMonitorPriorityPoll** and **SystemMonitorPriorityPollDuration** to determine how the System Monitor interacts with the tasks sent to it.
SystemMonitorPriorityPoll	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. This value is measured in milliseconds; the minimum value is 3000.The higher this number can be set, the more network traffic is avoided. This value is used with **SystemMonitorNonPriorityPoll** and **SystemMonitorPriorityPollDuration** to determine how the System Monitor interacts with the tasks sent to it.
SystemMonitorPriorityPollDuration	The value of this setting determines how long the System Monitor will remain in Priority Polling Mode. By default, the System Monitor regularly polls the AppServer using the milliseconds defined for the **SystemMonitorNonPriorityPoll** value. This **Non-Priority Mode** 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 **Priority Polling Mode.** While in Priority Polling Mode, the System Monitor polls the AppServer using the milliseconds defined for the **SystemMonitorPriorityPoll** value. 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. This value is used with **SystemMonitorNonPriorityPoll** and **SystemMonitorPriorityPoll** to determine how the System Monitor interacts with the tasks sent to it.

XML Tag	Purpose and Expected Value
UserID	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 **Single Sign On** feature and the current user selects the **Automatically sign on** check box on the **Preferences** window. For more information about how to activate this feature, review the **Single Sign On (Epicor Accounts)** section in the **System Administration Guide**.

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	This setting determines whether to clear the local client directory before a client update. Available options: • **Never** - The local client directory is never cleared. • **Always** - Clears the local client directory if core or custom deployments are updated. • **Core** - Clears the local client directory if the core deployment is updated. It does not clear the directory if only custom deployments are updated. • **Prompt** - Asks users if they want to clear the client directory whenever the core or custom deployments are updated.
clearDNS	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\<appserver_and_port> or the directory specified by alternateCacheFolder is conditionally cleared based on the value you enter for this setting. Available options: • **Never** • **Always** • **Prompt**

XML Tag	Purpose and Expected Value
DeploymentServer	The URI of the deployment directory on the deployment server.
deploymentPackage	If the setting of **deploymentType** is defined as "zip," the value of this setting is the name of the **zip** file retrieved from the Deployment Server during a client update. The default value is: ReleaseClient.zip
deploymentType	The method the deployment system uses to do actual deployment of client assemblies. The choices are **xcopy** and **zip** (which copies a named zip file locally and then unzips).
doDateComparison	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. The choices are **true** (the default) or **false**. If it is set to false, then xcopy copies all files regardless of modification date.
optimizeAssemblies	A setting that determines whether you can optimize assemblies within the Epicor application. The choices are **true** or **false**. A setting of true requires that you have admin rights on the client installation.

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	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. 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 **Epicor Help URL** field.

XML Tag	Purpose and Expected Value
AnnotationsOverrideXSL	The **path** or **file name** 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.
courseServer uri	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/" 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 **Education Courses URL** field. 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.
E9EducationKeysServer uri	If the URL changes for **Education Courses License** 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.
featureSummaryHomePage	The web page that is to serve as the home page for the Feature Summary.
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 " **Epicor Applications**" followed by the URL href = " **http://eportal.epicor.com**"

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	This value indicates the method that will be used globally to sort strings within the application. The available values are:

XML Tag	Purpose and Expected Value
	stringSort – 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. **wordSort** – 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. To change the global default value for the application, use the following syntax: `<stringSort value="default" /> <wordSort value="default" /> >`

Sort Method Exceptions	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 ("**TableName.ColumnName**") 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 (<wordSort value="default" />) that indicates the stringSort method that will be used on part numbers. This exception value uses the following syntax:
	
	<stringSort value="Part.PartNum" />
	
	Each exception line only supports one table/column combination. To apply this logic to multiple table/columns, enter multiple lines:
	`<stringSort value="Part.ParNum"/>`
	
	`<stringSort value="Customer.CustNum"/>`
	
	Continue to enter all the exception lines that you need.
	
	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.

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 **HELP**	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.
AUTOLOADSUPPRESS	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.
BASE	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.
CLASSIC	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.
CONFIG=<filename>	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
CRM	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: • Customer Relationship Management • Case Management • Quote Management • Configurator Management • ShopVision • Trackers

ARGUMENT	PURPOSE
	• Status Dashboards
DB	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.
HH	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.
HHC	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.
MES	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.
MESC	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.
MENUID=<Menu ID>	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 **Important** The MENUID run time argument only works with the Classic Style interface. It does not restrict menu access in the Modern Shell interface.
RPT	This argument applies only to Crystal Reports. It has no affect when printing SSRS reports. 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. Use this argument when you need a specific printer, like a label printer, to print out a specific report.
SHELL	This argument causes the application to launch using the Modern Shell interface. Users navigate the interface through tile groups that contain related programs.
SKIPCHECK	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. 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.
TE	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.

ARGUMENT	PURPOSE
UPDATE	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. 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.

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.

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.

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. **Interval** - This pattern handles all schedules shorter than a daily schedule. Enter the time between each run of this schedule. You can define the hours, minutes, and/or seconds time span between which this schedule will run.

   b. **Daily** - Select the check boxes of the days of the week on which the schedule runs.

   c. **Weekly** - Indicate how often the schedule should run, such as every 2 weeks. Then select the day of the week on which it should run.

   d. **Monthly** - You can indicate the schedule should run on a specific day of the month (for example, Every 15th), or select on which week and day in the month it should run (for example, The Last Saturday).

5. Now enter the date on which you want this schedule to activate in the **Next Run** field. You can either enter this date directly or click the **Down Arrow** to display the **Calender** and select a 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 you launched from your client. Depending on the permissions on your user account, you may also see additional tasks. 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.
- **Reports** - This displays all report/form programs which have run. All report programs (running on the application server) generate physical files. These files are the data source the System Monitor (running on the client) uses to perform the actual printing. The TaskAgent (also running on the application server) runs a purge of the reports approximately every 15 minutes. To keep a specific report file available for a longer length of time, use the **Archive Period** field on the report/form program. When you enter a value in this field, the TaskAgent does not purge it until the system clock passes this defined Archive Period value.

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:

- 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 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 comparing 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.

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

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 (EWA)

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 stop and start Internet Information Services (IIS). To do this:

1. Go to your server machine.
2. Log into the web server using an administrator account.
3. On the Windows desktop, click the **Start** button
4. Select **Run**. This displays the **Command Prompt** window.
5. Type **IISRESET** and then press your **<Enter>** button.

The Command Prompt window displays several messages that describe the reset process. When IIS is reset, a message displays indicating IIS is started again. 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.

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. For the
6. Between the double-quotes (" ") for this setting, enter the name (between the double quotes) of the server where you installed the Crystal Reports Embedded Server component. Typically this is the same server on which you installed EWA.
7. **Save** the file.
8. **Close** Notepad.
9. You next must stop and restart Internet Information Services (IIS). On the Windows desktop, click the **Start** button.
10. Select **Run**.
11. Enter **IISRESET** and then press your **<Enter>** button.

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. You next must stop and restart Internet Information Services (IIS). On the Windows desktop, click the **Start** button.
9. Select **Run**.
10. Type **IISRESET** and then press your **<Enter>** button.

IIS stops and then restarts. 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. You next must stop and restart Internet Information Services (IIS). On the Windows desktop, click the **Start** button.
9. Select **Run**.
10. Type **IISRESET** and then press your **<Enter>** button.

IIS stops and then restarts. 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. You next must stop and restart Internet Information Services (IIS). On the Windows desktop, click the **Start** button.
9. Select **Run**.
10. Type **IISRESET** and then press your **<Enter>** button.

IIS stops and then restarts. 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**.
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**

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**

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**

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.

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 this workshop, 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.

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.

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.

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. You update user accounts in **User Account Security Maintenance**. On the **Options** sheet, verify the the **Can Create Solutions** check box is selected.

Menu Path: System Setup > Security Maintenance > User Account Security Maintenance

Important This program is not available in Epicor Web Access.

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 Report(s)

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 Report(s)

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. You update user accounts in **User Account Security Maintenance**. On the **Options** sheet, verify the the **Can Install Solutions** check box is selected.

Menu Path: System Setup > Security Maintenance > User Account Security Maintenance

Important This program is not available in Epicor Web Access.

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. You can find these .pdf guides in the following EPICWeb locations:

- **EPICWeb > Downloads > 10.1**
- **EPICWeb > Documentation > Release [Current Release Number]**

To access these web sites, you must enter your EPICWeb account name and password.

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 **Epicor ERP 10.X Upgrade Guide** (Where 10.X is the current release number) 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 link:

- **Epicor ERP 10.x Release Upgrade Guide** - http://epicnet/sites/pdc/PreRelease_20Documentation/Epicor10_ReleaseUpgradeGuide_100to1013001.pdf

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.

Schema Changes

The database schema is the structure of the tables that make up the Epicor ERP database. 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**

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 **Epicor ERP 10.X.XXX Upgrade Guide** (where 10.X.XXX 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 link:

- **Epicor ERP 10.x Upgrade Guide** - http://epicnet/sites/pdc/PreRelease%20Documentation/Epicor10_UpdateGuide_1013002.pdf

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.

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

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 then 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 (IMInvc 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.

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

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.

You can review the transactions this process generates through a log. The log records the following time stamps:

```
09:40:53 Backflush Labor Server Process - Started
       09:40:53 Backflush Labor Server Process - Processing
       09:40:53 Backflush Labor Server Process - Completed
       09:40:53 Backflush Labor Server Process - Stopped
```

Log Options

Available logging options:

- **Log Filename** - The default file name is **BackFlushLaborProcess.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 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 PcInValues Log

Use the Convert PcInValues process to run your saved input values history (PcInValue 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 PcIn 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 Unlock Batch program from these menu locations:

Menu Path: Sales Management > Configurator Management > General Operations > Convert PCInValues

Menu Path: System Management > Rebuild Processes > Mfg / Distribution > Convert PcInValues

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 exists 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 processer 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 busier 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; Del
ta 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 finishing 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 processer identifier (PID). Then open the AppServer log and find the entry recorded an hour before the "Abandoned" error on the AppSever 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.
- If you see a **SQL Deadlock** error, launch the SQL Deadlock graph. Use the "HostPIDs" in the graph to find the PIDs in the AppServer log involved in the deadlock.

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: System Management > Upgrade/Mass Regeneration > Refresh PartBin QOH From PartTran

Menu Path: 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 provides counts of inbound and outbound records being handled by the Enterprise Configurator Server Process.
  - **Verbose** logging level has the same logging as Basic with additional logging for each individual message in the Enterprise Configurator Server Process, as well as a copy of the inbound and outbound XML document saved to disk.

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 provides counts of inbound and outbound records being handled by the Enterprise Configurator Direct Server Process.
  - **Verbose** logging level has the same logging as Basic with additional logging for each individual message in the Enterprise Configurator Direct Server Process, as well as a copy of the inbound and outbound XML document saved to disk.

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 provides counts of inbound and outbound records being handled by the Multi-Company Server Process.
  - **Verbose** logging level has the same logging as Basic with additional logging for each individual message in the Multi-Company Server Process, as well as a copy of the inbound and outbound XML document saved to disk.

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 provides counts of inbound and outbound records being handled by the Multi-Company Direct Server Process.
  - **Verbose** logging level has the same logging as Basic with additional logging for each individual message in the Multi-Company Direct Server Process, as well as a copy of the inbound and outbound XML document saved to disk.

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 subsquently 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 **RemoveOrphanedPickedOrdsMtlQueue.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**.

Salesperson

Displays the name of the salesperson who made the call.

Ship To/Contact

Displays the name of the contact at the customer/prospect site with whom the call took place. If you need to search for the contact ID, click the **Ship To/Contact** button to find and select the record you need.

Tip To send an e-mail to the contact, right-click over this field, and select **Email**. An email window displays and the To field populates with the e-mail address of the contact. To copy the text of the call to the email note, highlight the **Details** text of the call, right-click, and select **Copy**. Then in the e-mail note, insert the cursor, and press **Shift-Insert**. Your text is inserted. Additionally, you can attach a file to an outgoing e-mail. The record is attached to the CRM call as if it was added to the call record.

E-Mail/Phone/Fax

Displays any additional information for this contact. You cannot edit this information, it only displays for your review.

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 ans 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.

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**.

   Tip If a change log is being generated for a current file, a star displays on the Change Log button.

2. 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.

3. 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.

4. 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.

5. 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 be 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, Unliked 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 the **Mfgsysdata/Reports** directory. 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 are 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
Abort	Log entry generated when a user aborts processing of an inbound EDI transaction file using the Service Connect Task Monitor.
BlankDates	Log entry generated when blank Need By and Ship By dates are identified in the Main_DemandScheduleUpdate workflow.
CTPDates	Log entry generated when an attempt is made to update CTP Ship By or Need By dates.
DemandDetUpdate	Log entry generated for errors identified when updating the DemandDetail table in the Epicor application cannot be updated by the Main_DemandDetailUpdate workflow.
DemandHedUpdate	Log entry generated when the DemandHead table in the Epicor application cannot be updated by the Main_DemandHeadUpdate workflow.
DemandSchUpdate	Log entry generated for errors identified when updating the DemandSchedule table in the Epicor application cannot be updated by the Main_DemandScheduleUpdate workflow.
InvalidContract	Log entry generated when an invalid contract is identified in the Main_DemandHeadUpdate workflow.
InvalidDocument	Log entry generated when an invalid document is identified in the Main_DemandHeadUpdate workflow.
InvalidPart	Log entry generated when an invalid part is identified in an inbound EDI transaction file by the Main_DetailPartValidation workflow.

Error Code	Description
InvalidRevision	Log entry generated when an invalid part revision is identified an inbound EDI transaction file.
InvalidShipTo	Log entry generated when an invalid ship to customer code is identified in the Main_DemandScheduleUpdate workflow.
LeadTimeAdd	Log entry generated when a request is received on an inbound EDI transaction to add a demand schedule and it falls within the **Add** lead time window.
LeadTimeCancel	Log entry generated when a request is received on an inbound EDI transaction to change a demand schedule and it falls within the **Change** lead time window.
LeadTimeChange	Log entry generated when a request is received on an inbound EDI transaction to cancel a demand schedule and it falls within the **Cancel** lead time window.
LeadTimeDateChange	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 **Date Change** lead time window.
LeadTimeNewLine	Log entry generated when a request is received on an inbound EDI transaction to add a new demand line and it falls within the **New Line** lead time window.
LeadTimeQtyChange	Log entry generated when a request is received on an inbound EDI transaction to change a demand schedule quantity and it falls within the **Quantity Change** lead time window.
LockedDemand	Log entry generated when locked demand is identified in the Main_DemandHeadUpdate workflow.
PartialShipments	Log entry generated when an attempt is made to update a sales order release that has been been partially shipped.
PriceDiscrepancy	Log entry generated when comparing the price received on an inbound EDI transaction file, when compared to the Internal price.
Resubmit	Log entry generated when a user resubmits an inbound EDI transaction file for reprocessing using the Service Connect Task Monitor.
UnpostedDemandOnFile	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 are 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 PcInValue 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.

Global Alert Message Error Log

The Global Alert Error Log tracks issues that occur with global alerts.

Alert errors occur whenever the application is unable to send a global alert to a specified recipient. When such an error occurs, the application places an entry in the Alert Error log.

For example, if you trigger an alert but your email client software is not started, the application places an entry in the alert error log. If any entries are in this log and you have security rights to this log, you are notified of the entries when you first sign in.

If you activate global alerts, this log generates automatically. You use the Global Alert Error Log window to locate the error log entries.

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

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.

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.

Write Full DataSet

Select this check box to record the entire dataset content (f 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.

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.

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. Examples of these methods include Credit Checking, Part Verification and Pricing, and GetNewXXX (where XXX is the name of a record).

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.

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

   Important This program is not available in Epicor Web Access.

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 if you want to record all header and detail information within the tracing log. If this option is not selected, only header information is stored within the log.
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.

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.

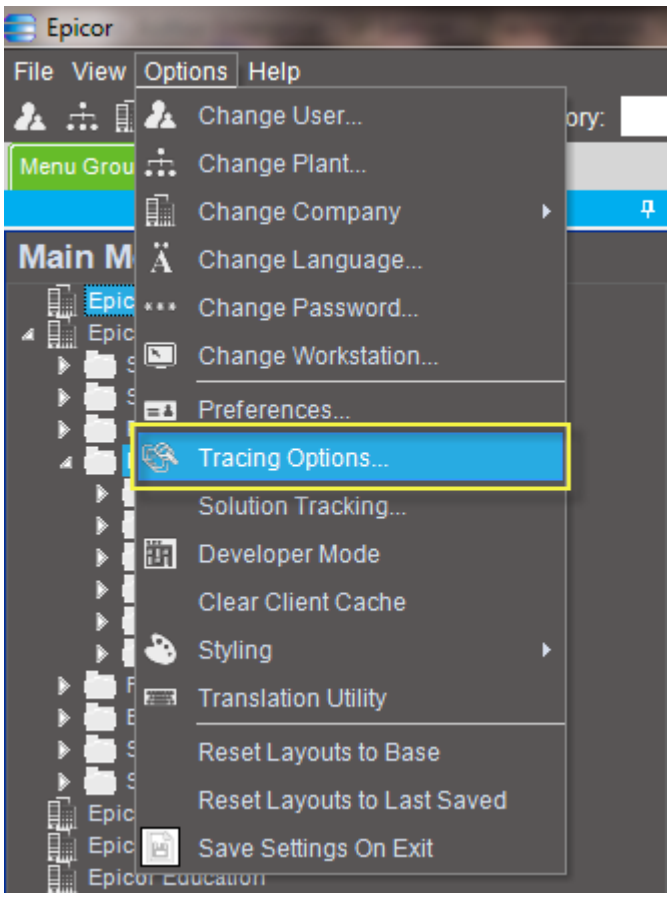
Activate From Client

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.

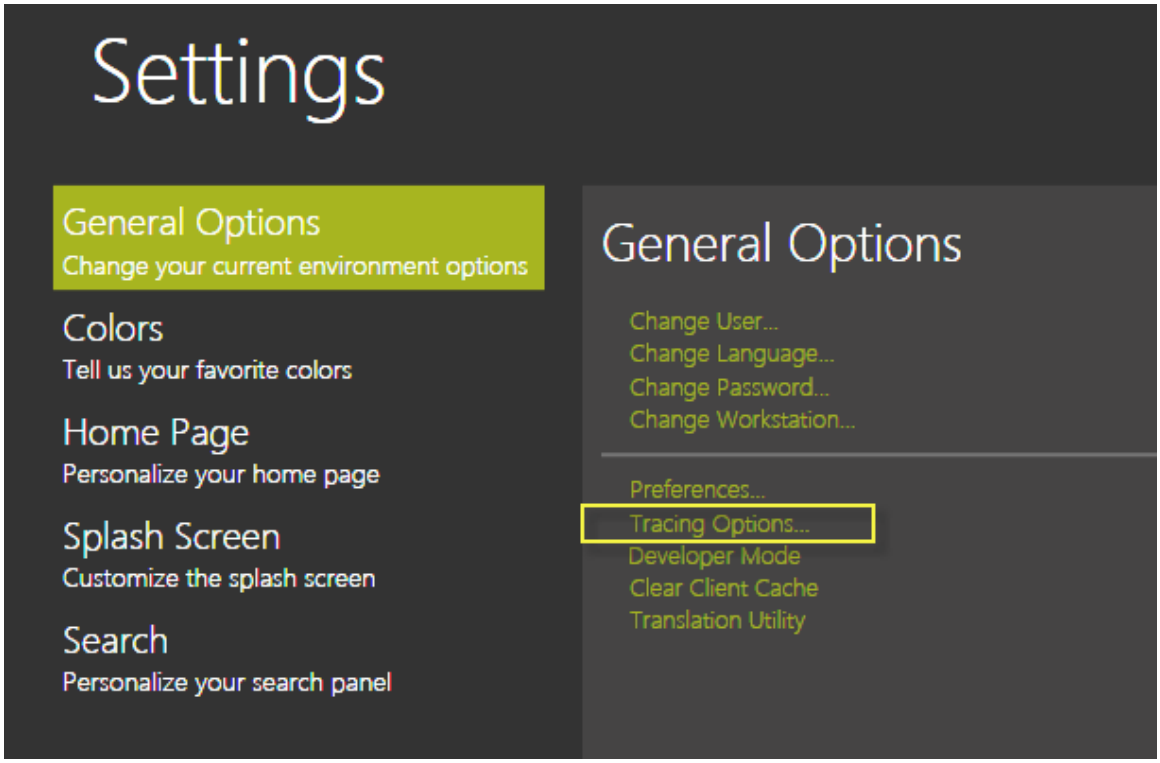
1. Launch the **Tracing Options Form**. Depending on interface style, you launch this window in different ways:

   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 Shell** 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**.



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 if you want to record all header and detail information within the tracing log. If this option is not selected, only header information is stored within the log.

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. 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.

6. 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.

7. 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.

8. Click the **Apply** to confirm your changes.

9. 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
<businessObject>	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.
<methodName>	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.
<returnType>	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.
<localTime>	The date and time stamp when the method was run.
<executionTime>	How long it took the method to run in milliseconds.
<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
Utc	The time the call was received in UTC time.
act	The message action (indicates the service and method being called).
dur	The duration of the server call in milliseconds.
cli	The IP address of the calling client. "::1:XXXXX" indicates the call was made from the same machine as the server.
usr	The identifier of the calling user.
tid	The thread ID assigned to handle the call.

Type	Description
pid	The server process ID.

3. Scroll through the log to see all the trace packets you activated.

Example

```
<tracePacket>
  <businessObject>Erp.Proxy.BO.PartImpl</businessObject>
  <methodName>GetList</methodName>
  <returnType>PartListTableset</returnType>
  <localTime>11/10/2013 12:07:42:7972865 PM</localTime>
  <executionTime>304</executionTime>
  <parameters>
    <parameter name="whereClause" type="System.String"><![CDATA[InActiv
e=false BY PartNum]]></parameter>
    <parameter name="pageSize" type="System.Int32"><![CDATA[100]]></par
ameter>
    <parameter name="absolutePage" type="System.Int32"><![CDATA[0]]></p
arameter>
    <parameter name="morePages" type="System.Boolean"><![CDATA[False]]>
</parameter>
  </parameters>
  <serverTrace>
    <Op Utc="2013-10-11T10:08:06.5227429Z" act="Erp:BO:Part/PartSvcCont
ract/GetList" dur="15.842" cli="10.66.8.121:56292" usr="manager" machin
e="HVW12AS09" pid="628" tid="127" xmlns="">
      <DBStatement type="PlantConfCtrl" duration="3.0122" rowCount="1"
hashCode="-4339069373789495130" dbContextId="37bbe39b-58e2-47b2-b694-4f
b6f0275ff8"></DBStatement>
      <Sproc name="[Erp]._ZFW_Part_GetList" duration="6.832400000000000
7"></Sproc>
      <RowEvent table="PartList" method="GetListRowLoaded" rows="100" d
uration="0.0175"></RowEvent>
      <Expression hc="-4339069373789495130">(ctx, CompanyId, iPlant) =&
gt; Queryable.FirstOrDefault(Queryable.Where(
  ctx.PlantConfCtrl,
  row =&gt; row.Company == CompanyId &amp;&amp; row.Plant == iPlant
))</Expression>
    </Op>
  </serverTrace>
</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,ESENotificationSourceID]]></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.

Database Migration Log

During the upgrade process, you most likely will also migrate your database(s) to the current version. This ensure 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.

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 when you are experiencing performance issues.

The BAQs fields can improve how business activity queries gather data and run on your system; use these fields to optimize query processing. You activate and configure the application server log to help determine the cause of slow performance. You can then display this log within the Performance and Diagnostic Tool or send this log to Epicor Technical Support or your Epicor consultant.

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.

Remember when you change the application server settings on this window, you will cause the application server to restart. Be sure to change these settings during a period of the day when few users are logged into the Epicor ERP application.

1. From either the **Action** menu or the **Actions** pane, select **Application Server Settings**.

   The **Application Server Settings** window displays.

2. For the **BAQ Query Max Result Rows** field, enter the highest number of rows a business activity query can return.

   By entering a value in this field, you restrict how many rows can be pulled for display by each BAQ. This prevents the query from pulling in an unlimited number of records, restricting situations where a runaway BAQ consumes too many system resources to generate query results The default value is 0, indicating there is no limit.

3. 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.

4. You then use the rest of the fields on this window to activate the application server log and determine what information this log gathers. Select the **Trace Log Enabled** check box.

5. 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.

6. 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**

7. 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.

8. 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. 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.

   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. **Detailed Exceptions** - Indicates you want to record the complete details of each exception message. The full stack trace of the exception is included in the server log. You then see which items in your Epicor ERP application were affected by the exception.

   d. **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.

   e. **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.

   f. **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.

9. 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.

10. When you finish making your selections, click **Apply** and then **OK**.

11. 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**.

The application server restarts, using the selected BAQ parameters and trace log options. Your selected trace log settings are written to the **AppServer.config** file. 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 located in the **DeploymentServer** 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 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

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

   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

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 in a log you can review 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.

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.

   Tip Events generated before the 3.0.5.0 version will have EpicorICETaskAgentService as their source. If the events were generated by the 3.0.5.0 version or later, their source will be EpicorTaskAgent3.0.5.0, EpicorTaskAgent3.0.6.0, and so on.

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. When you finish reviewing the events, click the **Close** button.

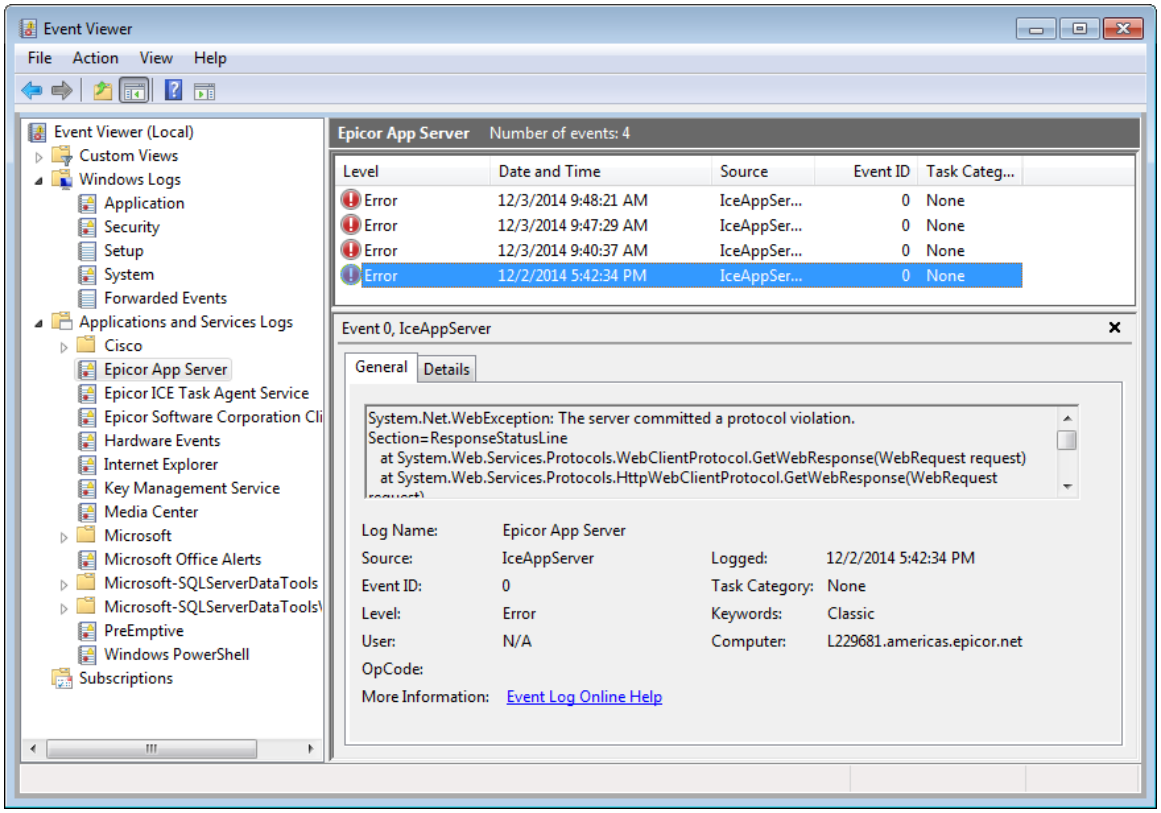
Event Viewer

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.

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.

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 (EWA) 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

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

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

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

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
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 that 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

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, restart Internet Information Services (IIS):

1. Log into your server machine.
2. Launch the **Windows® PowerShell®**.
3. At the command prompt, enter **IISRESET** and press **<Enter>**.
4. After IIS stops and restarts, close **Windows® PowerShell®**.
5. Log into the Epicor ERP application.

6. 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
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.
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 **EpicorSupport** 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.

Checklist Item	Task to Complete
Gather Main Details	Create a document that contains your **Site ID**, **Company Name**, **Call Number**, and the **Epicor Version**.
Gather Issue Details	Answer a series of questions about the issue and create the steps to duplicate.
System Information	Run the **msinfo32** 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 **Epicor Task Agent Service [CurrentVersionNumber]** folder and any **Setup Configuration** 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

   Important This program is not available in Epicor Web Access.

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**:
   - When you run the application using the **Classic Style** (Epicor 9.xx style), on the Main menu, from the **Options** menu, select **Developer Mode**.
   - When you run the application using the **Modern Shell** (Epicor 10.xx style), click the bottom arrow to display the toolbar; select the **Developer Mode** (wrench) button.
   - Alternately in the **Modern Shell** menu, click the **Settings** tile; from the **General Options** list, select the **Developer Mode** option.

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(s)

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.

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 **Problem 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 Problem 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, enter **psr**.

5. From the search results, select the **Record steps to reproduce a problem** option.
   The **Problem 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 Problem 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

Important This program is not available in Epicor Web Access.

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. Launch the **Tracing Options Form**. If you use the **Classic Menu**, click **Options > Tracing Options**. If you use the **Modern Shell Menu**, click the **Down Arrow** at the bottom of the window to display the toolbar, then click the **Tracing Options** button.

b. Select the **Enable Trace Logging** check box.

c. Select the tracing options you need.

d. 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://ftpmpls.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.

Index

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

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.