



Epicor Service Connect Installation and Implementation Guide

Epicor 10

Disclaimer

This document is for informational purposes only and is subject to change without notice. This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication. However, Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims any applicable implied warranties, such as fitness for a particular purpose, merchantability, satisfactory quality or reasonable skill and care. As each user of Epicor software is likely to be unique in their requirements in the use of such software and their business processes, users of this document are always advised to discuss the content of this document with their Epicor account manager. All information contained herein is subject to change without notice and changes to this document since printing and other important information about the software product are made or published in release notes, and you are urged to obtain the current release notes for the software product. We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice. The usage of any Epicor software shall be pursuant to an Epicor end user license agreement and the performance of any consulting services by Epicor personnel shall be pursuant to Epicor's standard services terms and conditions. Usage of the solution(s) described in this document with other Epicor software or third party products may require the purchase of licenses for such other products. Where any software is expressed to be compliant with local laws or requirements in this document, such compliance is not a warranty and is based solely on Epicor's current understanding of such laws and requirements. All laws and requirements are subject to varying interpretations as well as to change and accordingly Epicor cannot guarantee that the software will be compliant and up to date with such changes. All statements of platform and product compatibility in this document shall be considered individually in relation to the products referred to in the relevant statement, i.e., where any Epicor software is stated to be compatible with one product and also stated to be compatible with another product, it should not be interpreted that such Epicor software is compatible with both of the products running at the same time on the same platform or environment. Additionally platform or product compatibility may require the application of Epicor or third-party updates, patches and/or service packs and Epicor has no responsibility for compatibility issues which may be caused by updates, patches and/or service packs released by third parties after the date of publication of this document. Epicor® is a registered trademark and/or trademark of Epicor Software Corporation in the United States, certain other countries and/or the EU. All other trademarks mentioned are the property of their respective owners. Copyright © Epicor Software Corporation 2014. All rights reserved. No part of this publication may be reproduced in any form without the prior written consent of Epicor Software Corporation.

Epicor 10

Revision: July 24, 2014 5:47 a.m.

Total pages: 23

sys.ditaval

Contents

1 Getting Started.....	4
1.1 Introduction to Epicor Service Connect.....	4
1.2 Hardware and Software Requirements.....	5
1.2.1 Hardware Requirements.....	5
1.2.2 Epicor Service Connect Server Software Requirements.....	6
1.2.3 Epicor Service Connect Client Software Requirements.....	7
1.2.4 32-bit vs 64-bit Installation.....	8
2 Installation and Configuration.....	9
2.1 Upgrade to Epicor Service Connect 10.....	9
2.2 Install Epicor Service Connect Server.....	10
2.2.1 Uninstall Epicor Service Connect Server.....	10
2.2.2 Install Epicor Service Connect Server.....	10
2.2.3 Install Epicor Service Connect Server on Windows 2008/2012 Server.....	13
2.3 Install Epicor Service Connect Client.....	14
2.3.1 Before You Begin.....	14
2.3.2 Install Epicor Service Connect Client.....	15
2.4 Configure Epicor Service Connect DCOM.....	16
2.4.1 Verify DCOM Configuration Prerequisites.....	16
2.4.2 Configure DCOM Security Limits.....	16
2.4.3 Additional Configurations.....	17
2.4.4 Configure Epicor Service Connect Client.....	18
2.4.5 Set the Sharing and Security Model to Classic.....	18
2.4.6 SQL Server.....	19
2.5 Epicor 9.0 Web Services.....	19
2.6 Epicor Service Connect Task Monitor.....	20
2.7 .NET Extensions.....	20
2.8 SharePoint Component	20
3 Implementation.....	21
3.1 Concepts.....	21
3.2 Processes.....	21
3.2.1 Register Documents.....	22
3.2.2 Import Web Services.....	22
3.2.3 Set Up Communication Channels.....	22
3.2.4 Create Workflows.....	22
3.2.5 Set Up Message Map.....	22

1 Getting Started

Welcome to the Epicor Service Connect Installation and Configuration Guide - Version 10.

This part of the guide explains how to verify the prerequisites prior to installing Epicor Service Connect.

1.1 Introduction to Epicor Service Connect

Epicor Service Connect provides a powerful and flexible environment to support specific collaborative processes, connecting different business entities, applications or users.

Epicor Service Connect consists of four major parts: Service Connect Framework, Tools, Task Monitor and Administration Console. These components can be used to create and run custom, flexible workflows that accept different formats of data and allow processing of this data using various services available with web-service technology.

Service Connect Framework

Service Connect Framework is a group of system services that provides main system activities like running communication channels, executing workflows, tracking of documents and system events.

Tools

A group of tools that help to configure system framework, workflows and document types.

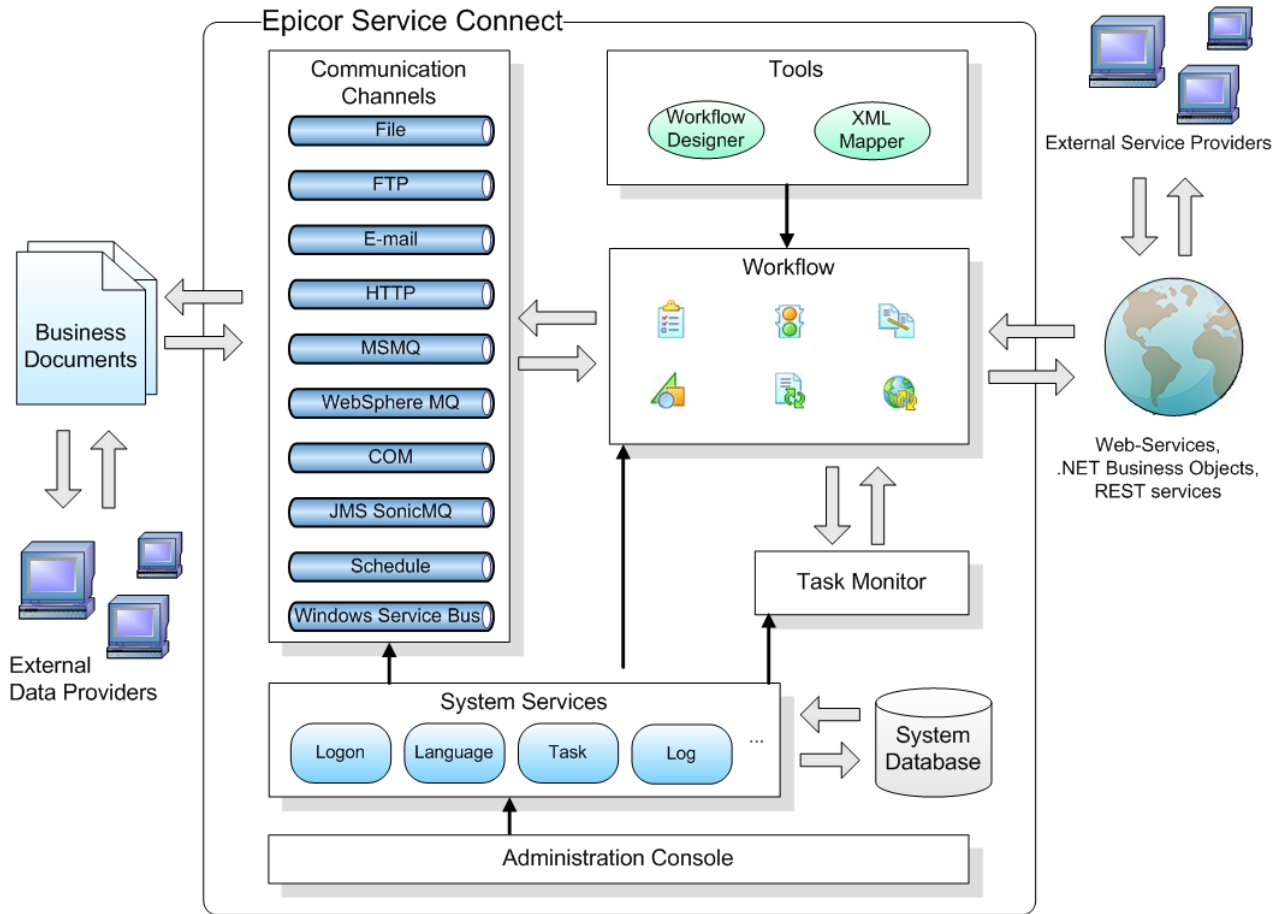
Task Monitor

Task monitor is a web interface intended to view, track and process user tasks that are assigned during workflow execution.

Administration Console

The Service Connect Administration Console is Microsoft Management Console (see Microsoft's overview) and is used to configure and maintain settings for Service Connect Framework services.

The following graphic shows an architectural overview of the system:



Important Do not install Service Connect {Standalone} on top of an existing iScala installation. Service Connect for iScala is installed as part of iScala package.

Service Connect {Standalone} package is created to install Service Connect on a server separate from iScala in order to use SC with other systems (Epicor, Vantage, E4SE, etc.).

1.2 Hardware and Software Requirements

Review the minimum and recommended hardware and software requirements for Epicor Service Connect installation.

1.2.1 Hardware Requirements

Review recommended system requirements:

- Intel Core 2 Duo starting from 2.4 GHz or better
- 4 GB RAM or more
- Gigabit network connection.
- DVD drive.

1.2.2 Epicor Service Connect Server Software Requirements

Review recommended server software requirements:

Server Operating Systems

- Microsoft Windows Server 2008 Standard Edition SP2
- Microsoft Windows Server 2008 Enterprise Edition SP2
- Microsoft Windows Server 2008 R2 Standard Edition SP1
- Microsoft Windows Server 2008 R2 Enterprise Edition SP1
- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2012 R2 Standard Edition

Required Server Software

Database Management Systems (DBMS)

The following database management systems are supported:

- Microsoft SQL Server 2008 Standard Edition SP3
- Microsoft SQL Server 2008 Enterprise Edition SP3
- Microsoft SQL Server 2008 Express Edition SP3
- Microsoft SQL Server 2008 R2 Standard Edition SP2
- Microsoft SQL Server 2008 R2 Enterprise Edition SP2
- Microsoft SQL Server 2008 R2 Express Edition SP2
- Microsoft SQL Server 2012 Standard Edition SP1
- Microsoft SQL Server 2012 Enterprise Edition SP1
- Microsoft SQL Server 2012 Business Intelligence Edition SP1
- Microsoft SQL Server 2012 Express Edition SP1
- Microsoft SQL Server 2012 SP1 Native Client.

The required redistributable package is provided in ESC Setup package. ESC setup installs appropriate package, if it is not found on the workstation.

- Microsoft SQL Server 2014

Epicor Service Connect supports any configuration of Microsoft SQL Server:

- SQL Server 2008 x64 and x86 are supported
- SQL Server 2012 x64 and x86 are supported
- SQL Server 2014 x64 and x86 are supported
- All collation types for the SQL server are supported: any dictionary order, character set, case-sensitive and case-insensitive search.

The following software is required as well:

- Microsoft Internet Information Services (IIS) 7.0, 7.5, or 8.0 (Common files and WWW Service are required, SMTP and FTP are optional)
- Microsoft Message Queuing Services (MSMQ) 2.0 (optional).
- IBM WebSphere MQ Server or Client 5.1 (or above) (optional, English language only).
- SonicMQ v7.6 CSharp Client for Windows (optional)

- Windows Service Bus 1.0 (optional)
- Microsoft .NET Framework 4.5 (full) must be installed.

Epicor Service Connect setup does not install the package if it is not found on the system.

- Microsoft Web Services Enhancements (WSE) 2.0 SP3 is a prerequisite for Epicor Service Connect. It is shipped with ESC and installed if needed at the beginning of ESC installation. To be installed successfully, WSE needs Microsoft .NET Framework 1.1 as a prerequisite.

Even if a different version of WSE is already installed, you should install Microsoft Web Services Enhancements (WSE) 2.0 SP3.

- Microsoft XML Parser (MSXML) 6.0 SP1. The required MSXML 6.0 SP1 redistributable package is provided in ESC Setup package. ESC setup installs appropriate package if it is not found on the system.
- One of the following internet browsers:
 - Microsoft Internet Explorer 7.0, 8.0, 9.0, 10 or 11. Typical set of components.
 - FireFox 25.0
 - Chrome 30.0.1599.101m
 - Safari 5.1.7

Integration between Service Connect and Windows SharePoint Services 2013, SharePoint Foundation 2013 and older versions are supported.



Note Epicor Service Connect installer does not add https binding in IIS. If there is no https binding, you need to add it manually. It is required to work with SCIntegration service (WCF version).



Important Epicor Service Connect installer (SC Server x86, SC Server x64, SC Client) will not work on a computer with iScala Server (x86/x64), iScala Client, iScala CRM (x86/x64), iScala WebPA, or Reporting Services Connector (x86/x64) installed. Service Connect standalone and iScala should not be installed on the same server at the same time, as this may lead to unpredictable behavior of the resulting installation.

iScala includes its own version of Service Connect, and therefore there is no need to install SC Standalone and iScala on the same machine.



Note

Third-party redistributables are NOT removed when ESC is uninstalled.

1.2.3 Epicor Service Connect Client Software Requirements

Review recommended client software requirements:

Workstation Operating Systems

The following workstation operating systems are supported:

- Microsoft Windows Vista (Business, Enterprise or Ultimate Edition) SP2
- Microsoft Windows 7 (Professional, Enterprise or Ultimate Edition) SP1
- Microsoft Windows 8 (Professional or Enterprise)
- Microsoft Windows 8.1 (Professional, Enterprise)



Note Client software for Epicor Service Connect cannot be installed on Windows 9x and Windows Millennium workstations.

Required Workstation Software

The following software should be installed on the workstation:

- One of the following internet browsers:
 - Microsoft Internet Explorer 7.0, 8.0, 9.0, 10 or 11. Typical set of components.
 - FireFox 25.0
 - Chrome 30.0.1599.101m
 - Safari 5.1.7
- Microsoft SQL Server 2012 SP1 Native Client. The required redistributable package is provided in ESC Setup package. ESC setup installs appropriate package, if it is not found on the workstation.
- Microsoft XML Parser (MSXML) 6.0 SP1. The required MSXML 6.0 SP1 redistributable package is provided in ESC Setup package. ESC setup installs appropriate package, if it is not found on the workstation.
- Microsoft .NET Framework 4.5 (full) must be installed. ESC setup does not install Microsoft .NET Framework, if it is not found on the workstation.

Microsoft .NET Framework 4.5 requires Windows 2008 or above on servers and Windows Vista or above on workstations

- To develop workflows using Windows Workflow Foundation, Visual Studio 2010 should be used; refer to Visual Studio 2010 documentation to learn more on how to develop WWF workflows.



Note Third-party redistributables are not removed during ESC un-installation.

1.2.4 32-bit vs 64-bit Installation

Service Connect media is available for both 32-bit and 64-bit installation. Please be sure to go to the appropriate folder according to your server.

At the moment all Epicor Web Services are certified only for 32-bit execution. In order to host Epicor Web Services and/or Service Connect on the same 64-bit Windows operating system, IIS should be modified (on the 64-bit system) to run in 32-bit execution mode, and the 32-bit Service Connect should be installed (see below).

IIS 7.0 or above

In IIS you can run 32-bit and 64-bit applications at the same time.

If you install 64-bit Service Connect version, you should set the application pool to 64-bit.

If you install 32-bit Service Connect version, you should set the application pool to 32-bit. To do this:

1. Navigate to Internet Information Services (IIS) Manager, and expand the list of Application Pools.
2. Right-click the **EpicorSCP** Application Pool and select **Advanced Settings....** Alternatively, you can select **Advanced Settings...** from the **Actions** pane after selecting the Application pool.
3. Set **Enable 32-bit Application** to True.
4. Click **OK**.
5. Restart Application Pool



Note You can use 64-bit Service Connect with Epicor9 Web Services.

2 Installation and Configuration

Epicor Service Connect has separate installation packages for SC server and SC client. If you want to install server and client on the same machine, start with server installation, and then you are prompted to continue with client installation. You can also install server and client on different machines.

The following features are installed with SC server:

- Framework (required)
- Web-Based Task Monitor (optional)
- Integration Services (optional)
- Integration Wcf Services (optional)

The following features are installed with SC client:

- Administration Console (optional)
- Developer Tools (optional)
- Tools (required)
 - Database Converter (required)
 - Service Manager (optional)
 - DesPoster (optional)
 - Workflow Converter (optional)
- Help (optional)
- Samples (optional)
- Shortcut for Task Monitor (optional)

2.1 Upgrade to Epicor Service Connect 10

If you use Epicor Service Connect, you must upgrade to the latest version. Use the following instructions to locate the installation instructions in order to upgrade to the latest version of Epicor Service Connect.

1. Logon to the EPICweb Customer portal. Navigate to **Products > Epicor ERP > Downloads. Expand Epicor Service Connect > Version 10.0.**
2. In the Available Downloads list, select and download the latest Epicor Service Connect installation zip file.
3. Extract the files. Navigate to the Documents folder to locate the Epicor Service Connect Installation Guide.
4. Use the guide to upgrade Epicor Service Connect.
5. After your upgrade, test your system to verify that Epicor Service Connect works successfully.

2.2 Install Epicor Service Connect Server

Use the following steps to install Epicor Service Connect Server.

2.2.1 Uninstall Epicor Service Connect Server

If a previous version of Epicor Service Connect exists on the server, use the following steps to uninstall it. The uninstallation process depends on the currently installed version of Service Connect.

- If SC 8.1, SC 8.2, or SC 8.3 had been installed, it needs to be uninstalled manually. To do this:
 1. Navigate to **Start > Control Panel > Programs > Uninstall a Program**.
 2. Select the Epicor Service Connect installation and click **Uninstall**.
 3. Verify that the uninstallation was completed successfully.
- If a Hotfix was installed on SC 8.1, binaries and registration will stay on the server.
- In most cases, SC installer properly cleans up the system, but it is highly recommended to control the cleanup during SC installation as explained below.

2.2.2 Install Epicor Service Connect Server

Use the following steps to install the Epicor Service Connect:

1. Insert the **Service Connect 10 Installation CD** into the server's DVD-drive.
2. Navigate to and open the **Service Connect Install** folder.
3. Double-click **Setup.exe**.
4. If SC 8.1 with HF was installed on the server, the SC 8.1 uninstaller will start automatically. When uninstallation is finished and the **Next** button is enabled, you should verify the system cleanup:
 - a. Open Windows Task Manager and verify that Sca* processes are not running.
 - b. Go to the installation folder of the SC 8.1 and verify that it does not contain any binary files (*.exe and *.dll). Any custom settings, like processes or channels, should not be removed.
 - c. Go to the common files folder and verify that it does not contain any binary files (*.exe and *.dll) in the Scala Business Solutions NV folder.

If one or more of these conditions are not met, uninstaller had failed to clean up the system. In this case, cancel the installation, start ScalaSystemCleaner.exe from the SC Installation CD and direct it to the location where SC 8.1 with Hotfix was installed. After ScalaSystemCleaner.exe finished system cleanup, start the SC 10 installation again.

5. In the **Welcome** window, click **Next**.
6. In the **License Service Setup** window set the following:
 - **Read *.lic license files from this folder**. Defaults to the path where from the installation program is launched. You can accept the default location or click the **Change** button to specify custom location.

Select this option, if you do not have server with license service of the Service Connect product installed yet.

- **Select a machine with installed License Service.** Defaults to the current machine. Select this option, if you already have a server with Service Connect License Service installed.

7. In the **Destination Folder** window, accept the default location or click the **Change** button to install the application to a custom location.
8. In the **Web Applications** window, select if you want to create SC web applications in a separate web site. If you select the **Create new web site for Epicor Service Connect 10 web applications** check box, a separate web site for SC is created. The **scshost** host header is assigned to it. The **BPMIntegrationService**, **Schemas**, **WorkflowWebServices**, and **TaskMonitor** web applications are added as subdirectories within this web site.

It is recommended to create new web site for SC, so that the virtual directories created by other applications do not conflict with SC virtual directories or the settings of the default web site do not conflict with SC requirements. To do this:

- a. In the **Web Applications** window, click **Next**. The installer checks if the web site with **scshost** HTTP host header (host header with any IP address, port **80** and name **scshost**) already exists.
- b. If the **scshost** web site exists, you are prompted to delete it.
 - Click **Yes** to delete **scshost** web site, and continue installation.
 - Click **No** to keep the **scshost** web site. In this case you can continue installation only if the **Create new web site for Epicor Service Connect 10 web applications** check box is clear. If this check box is selected, the **Web Applications** window is displayed again. To continue installation, either clear the **Create new web site for Epicor Service Connect 10 web applications** check box or select to delete the existing **scshost** web site.

If you keep the **scshost** web site, it may cause problems when working with SC. However, you can manually re-configure or delete the existing **scshost** web site.



Note Installation may fail, if the default web site does not have an empty host header in its bindings.

For example, if the default Web site in the IIS has just one header - 'scshost', and you run SC Installer, select installation Web Application to the Default site in the **Web Application** window, and then click **No**; the installation fails.

If the Default web site has both an empty host header and 'scshost' host header, the installation runs successfully.

9. In the **Choose Setup Type** window, select the setup type for the SC server. Available options:
 - **Complete.** All the features of SC server are installed.
 - **Custom.** You select, which of the SC server features to install. When selecting this option, you can also specify where the selected features should be installed. Installation of Framework is required, you cannot unselect this feature; specify whether you want to install **Web-Based Task Monitor** and **Integration Services**.
10. In the **Database Setup** window set the following:
 - **Create a new SC System database.** Select this option if you do not have system database installed yet, or if you want to recreate it. Note that in this case all data in the database will be lost.

The installer creates the two default ESC users: **Admin** and **Epicor**. The passwords for these users are empty by default. It is prompted to provide the passwords in the Default user passwords window. There are no limitations for the password length and format. The user names are fixed and cannot be changed.

These credentials (usernames and passwords) can be used when the user credentials are asked by ESC Administration Console. It is recommended to change the blank password during the installation or after the first logon.

- **Select an existing database.** Select this option if the system database already exists on the server and you want to preserve old settings. If your database version is different from the one being installed, the installer will suggest database conversion. It is possible to convert database either during the installation or later. Database is migrated with the SC Database Converter. To start SC Database Converter manually, run **<SC install directory>\Tools\ScaDBConvert\ScaDBConvConsole.exe**. It is recommended to back up database before upgrading it.



Note The user, who performs database conversion using SC Database Converter, is a trusted user. This user should be able to login to the system database being converted, and, in addition to that, this user should have db_owner rights for this system database. Otherwise, the Database Converter fails with an error.

- **Server Name.** The name of the SQL server. Defaults to the current machine.



Note The default installation of SQL Server Express creates an instance named SQLExpress. If you install Service Connect with SQL Server 2005 Express Edition, append the instance name to the server name (for example, myserver\SQLExpress) in order to complete the installation successfully; otherwise, the installation fails.

- **Database Name.** This is the database where Service Connect system information is stored. This data includes various system and administrative settings such as user accounts, communication channels and document tracking.
- **Use NT authentication.** If you select this option, the current login account must have access and necessary permissions in the SQL Server.
- **User Name.** Complete this field if you did not select to use NT authentication.
- **Password.** Complete this field if you did not select to use NT authentication.

11. In the **System Services Account** window, enter username and password for the domain user under whose account the system services will run. Note that the user must have appropriate rights to system database. You can leave fields empty. In this case **LocalSystem** account will be used instead; you can then manually set logon accounts after installation.

12. Click **Install**.

13. If you want to install SC Client on the same machine, select the **Run Client Setup** check box. In the case, client installation starts immediately after you clicked **Finish**. If you do not want to install client on the same machine, clear this check box. In both cases the client installation package is copied to **<install directory>\Client** folder, and you can install SC client from this folder at any time.

14. Click **Finish**.

15. If you are migrating from SC version older than ESC 8.3, relocate Customized Workflows and Email Templates. Move the Customized Workflows and Email Templates from the following folders:

- <SC Installation Folder>\System\Services\Workflow\Processes\Custom
- <SC Installation Folder>\System\Services\Workflow\EmailTemplates\Custom

to

- <SC Installation Folder>\System\Services\Des\Processes\Custom
- <SC Installation Folder>\System\Services\Des\EmailTemplates\Custom

16. If you are migrating from SC version older than ESC 8.3, and your system has processes that had been exposed as Web Services before migration to SC 10, you should manually move these Web Services (ScaWebServices/*.asmx) to the new location: **<SC Installation Folder>\WebApps\WorkflowWebServices**.
17. If you are migrating from SC version older than ESC 8.3, from Task Monitor, publish InfoPath forms to the new location: Task Monitor folder is moved to **<SC Installation Folder>\WebApps\TaskMonitor**.
18. If you are migrating from a previous version of Service Connect, and are also upgrading your Epicor installation to Epicor 10, upgrade your workflows containing references to the older Epicor installations using **WorkflowConverter.exe** tool, provided with the latest Service Connect release. You can find detailed instructions of how to use this tool in the Service Connect Online Help under the following heading: **Epicor Service Connect Documentation Kit > Using Epicor Service Connect > Workflows > Managing Workflow Processes in Workflow Designer > Workflow Converter and Epicor Service Connect Documentation Kit > Using Epicor Service Connect > How To's > Best Practices: Workflow Converter**.

2.2.3 Install Epicor Service Connect Server on Windows 2008/2012 Server

If Epicor Service Connect is installed on Windows Server 2008/2012, for proper functioning of ESC features that require IIS, the Metabase Compatibility component of IIS 6.0 should be installed.

1. To Install the Metabase Compatibility, navigate to **Add/Remove Windows Components** and select **IIS > Web Management Tools > IIS 6 Management Capability Feature**.
2. Enable the file server role. To do this:
 - a. Navigate to **Start > Administrative Tools > Server Manager**.
 - b. In the **Roles** menu, click **Add Roles**.
 - c. Select **File Services**.
3. Enable the application server role. To do this:
 - a. Navigate to **Start > Administrative Tools > Server Manager**.
 - b. In the **Roles** menu, click **Add Roles**.
 - c. Select **Application Server**.
 - d. Select the following role services:
 - Web Server (IIS) Support
 - HTTP Activation
4. Enable the WEB Server (IIS) role. To do this:
 - a. Navigate to **Start > Administrative Tools > Server Manager**.
 - b. In the **Roles** menu, click **Add Roles**.

- c. Select **WEB Server (IIS)**.
 - d. Select the following role services:
 - ASP .NET
 - ASP
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools
 - IIS 6 Management Console
 - Basic Authentication
 - Windows Authentication
5. Configure DCOM. The configuration is described in detail in the **Epicor Service Connect DCOM Configuration** chapter.
 6. Configure **Windows Firewall**.
 7. Restart IIS.

2.3 Install Epicor Service Connect Client

You can install ESC client on the same machine with ESC server immediately after the server installation. You can also install it on a separate machine either from the installation folder created during the server installation, or from the installation CD.

2.3.1 Before You Begin

Verify the following prerequisites before you install Epicor Service Connect client:

- ESC server should be installed. Without ESC server installed, you will not be able to install ESC client, as the client installation asks for the name of the machine, on which ESC server is installed.
- If you install ESC client on a separate machine from the <install directory>\Client folder created during the ESC server installation (but not from the installation CD), share the <install directory>\Client folder.
- If you install ESC in multiple domain environment (ESC server and ESC client are installed on different machines in different domains), trust relationship should be configured for these domains.

2.3.2 Install Epicor Service Connect Client

Use the following steps to install the Epicor Service Connect Client on a separate workstation.

1. Run **Setup.exe** from the <install directory>\Client folder, created by the server installer, or from the installation CD.
2. In the **Welcome** window, click **Next**.
3. In the **Logon Service Location** window, accept the default machine name or specify it manually to connect to the logon service to another computer.



Note If the client installation fails with the error message "Unable to connect to Logon service on the specified computer", then the Remote Activation permission for the ScaLogonSrv COM component should be set up on the server for the user, for which the ESC client is installed. To do this:

1. Click **Start** and select **Control Panel**.
 2. In the Control Panel, select **Administrative Tools > Component Services**.
 3. In the **Component Services** tree view, navigate to **Component Services > Computers > My Computer > DCOM Config** and select the **ScaLogonSrv** node.
 4. Right-click the **ScaLogonSrv** node and select **Properties**.
 5. In the **ScaLogonSrv Properties** dialog box, open the **Security** tab.
 6. On the **Security** tab, in the **Launch and Activation Permissions** section, select **Customize** and then click **Edit**.
 7. In the **Launch Permission** dialog box, in the **Group or user name** section, add or select the user for which you want to setup the Remote Activation permission, and in the **Permissions for <the selected user>** section, select the **Allow** check box next to the **Remote Activation** permission for this user.
 8. In the **Launch permission** dialog box and in the **ScaLogonSrv Properties** dialog box, click **OK**.
-
4. In the **Destination Folder** window, accept the default location or click the **Change** button to install the application to a custom location.
 5. In the **Choose Setup Type** window, select the setup type for the SC client. The following options are available:
 - **Complete**. All the features of SC client are installed.
 - **Custom**. You can select, which of the SC client features to install. When selecting this option, you can also specify, where the selected features should be installed.
 6. In the **Customer Information** window, enter your user name and the name of your organization. Click **Next**.
 7. Click **Install**.
 8. Click **Finish**.

To install SC Client in silent mode, use the following command line format:

```
msiexec /i "Epicor Service Connect Client.msi" /q /l*v %Temp%\client.log LOGONS  
RVHOST=ServerName
```

where **ServerName** is the name of the server with SC Server installed, and **%Temp%** is system variable, that keeps the path to the temporary folder specific for the currently logged in user. During installation in silent mode, all diagnostic information and errors are saved into log file, specified in the command line. Before installing SC Client in silent mode, make sure that .NET Framework is installed on the destination machine. Otherwise the silent mode installation cannot be accomplished.

When upgrading Service Connect to the next version, the SC Client Installer notifies about re-import of existing Web and .NET references.

2.4 Configure Epicor Service Connect DCOM

If Epicor Service Connect is deployed in the client-server configuration, several changes of the operating system configuration (for example, user permissions) on the server and client machines are required. The section describes the setup of permissions an end-user must have on a machine running ESC.

For authentication purposes ESC may use the account the end-user is logged in on the workstation. This is why the so-called Windows domain should be used. Otherwise the system services will not be able to recognize the user who tries to access them.

2.4.1 Verify DCOM Configuration Prerequisites

Verify the prerequisites before you proceed with configuration:

- ESC 10 does not support Windows 2003.
- Refer to Server Software Requirements for the supported versions of Windows Server.
- Service Connect client requires access to the following components over DCOM:
 - ScaDESRouter
 - ScaLogonSrv
 - ScaLogSrv
 - ScaTaskSrv
- You should add windows group/user that will run ESC client to the DCOM security permissions of the services mentioned above. The following permissions should be allowed for each component:
 - Local Launch and Remote Launch
 - Local Activation and Remote Activation
 - Local Access and Remote Access
- DCOM security limits should be configured to allow these settings.

2.4.2 Configure DCOM Security Limits

Use the following steps to configure DCOM security limits for Windows Server 2008/2012 machine:

1. Navigate to **Start > Control panel > Administrative Tools > Component Services**.
2. In the **Component Services** dialog, expand **Component Services > Computers > My Computer**.

3. Right-click the **My Computer** node and select **Properties** from the context menu.
4. Click the **COM Security** tab.
5. Add windows group/user that will run ESC client to **Access Permissions** and **Launch and Activation Permissions Limits**.
 - a. To assign the **Remote Access** and **Local Access** permissions, in the **Access Permissions** section, click the **Limits** button.
 - b. To assign the **Local Launch**, **Remote Launch**, **Local Activation**, **Remote Activation** permissions, in the **Launch and Activation Permissions** section, click the **Limits** button.
6. Permissions should be granted to the default account of the web applications. The default accounts depend on the version of IIS. So, depending on your IIS version, grant the **Local Access**, **Remote Access**, **Local Launch**, **Remote Launch**, **Local Activation** and **Remote Activation** permissions to IIS_IUSRS group.
7. Click **OK**.

2.4.3 Additional Configurations

Use the following steps to perform additional configurations:

1. Configure the Windows Firewall on the computer, where SC server is installed. To do this:
 - a. Navigate to **Start > All Programs > Accessories > System Tools > Security Center**.
 - b. In the **Windows Security Center**, click the **Windows Firewall** link.
 - c. Either disable the Windows Firewall on the **General** tab, or configure the proper list of exceptions on the **Exceptions** tab.
2. Set the sharing and security model to **Classic** (this option is default for Windows 2008). To do this:
 - a. Navigate to **Start > Control Panel > Administrative Tools > Local Security Policy**. The **Local Security Setting** dialog box is displayed.
 - b. In the left pane, click the **Local Policies > Security Options** node.
 - c. In the right pane, double-click **Network access: Sharing and security model for local account** policy. In the dialog box, select **Classic** from the drop-down list.
 - d. Click **OK**.
3. On Windows Server 2008 64-bit, Windows Server 2008 R2, Windows Server 2012 add Anonymous Logon to the COM default Access permissions and to the security limits of Access Permissions, giving Local Access rights.

2.4.4 Configure Epicor Service Connect Client

Use the following information to configure Epicor Service Connect Client:

- The account used for SC services and components should be included in the local Administrators group on the client machine. Otherwise, when the client tries to logon to SC, an error occurs (“License server unavailable”, etc.).
- It is strongly recommended to use domain user accounts for SC services.

However, if for some reason the local user account (not a local system account) is used, the following conditions should be met:

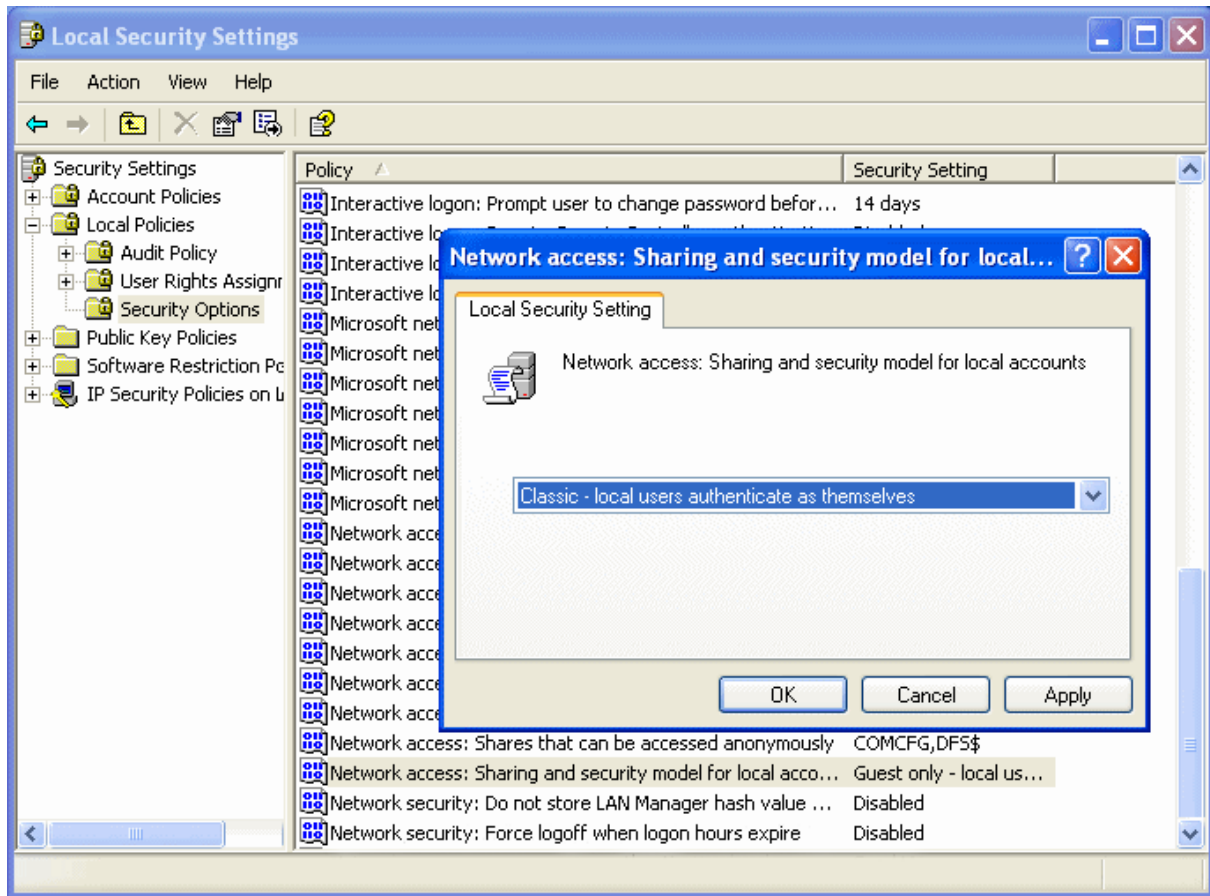
- The local account should exist on every client workstation. The password for this account should be the same on each workstation.
- For Windows 2008/2012 and Windows Vista, the sharing and security model should be set to Classic (default option for Windows 2008/2012). The steps for setting the sharing and security model are described below.

2.4.5 Set the Sharing and Security Model to Classic

Use the following steps, if you need to set the sharing and security model to Classic:

1. Navigate to **Start > Control Panel > Administrative Tools > Local Security Policy**. The **Local Security Setting** dialog box is displayed.
2. In the left pane, click the **Local Policies** node, and then the **Security Options** node.
3. In the right pane, double-click **Network access: Sharing and security model for local account policy**. In the dialog box, select **Classic** from the drop-down list.

4. Click **OK**.



2.4.6 SQL Server

If SC uses a server running on Windows 2008/2012 for the database, that server should have the same DCOM settings and permissions as the Application server for user account under which SC services are running.

Since SC services always access SQL server via trusted connection, the user account, under which they run, should have rights to access SC database.

2.5 Epicor 9.0 Web Services

To fully utilize Epicor Service Connect, you need to install the correct web services for your patch version of Epicor 9.0. The web services are delivered in the Web Services folder of each patch from 802 onwards. However, these are subject to updates when issues are found after patch creation.



Note WSE 3.0 is only required if you plan to implement WSE 3.0 policy types.

For detailed instructions on how to install WSE refer to the Reinstall Web Services section in the Epicor 10 Supplemental Install Guide.

2.6 Epicor Service Connect Task Monitor

The Task Monitor uses dedicated EpicorSCPool Application Pool. Starting from Service Connect 9.05.604, you should configure the Application Pool to use NET 4.0.

Verify the pool is not assigned to any other Web Epicor application, like EpicorServices. The EpicorServices should use another pool, usually DefaultAppPool, but not EpicorSCPool. Since IIS 7.0 can work with any pools (.NET 2 and .NET 4) simultaneously the EpicorServices web application can use any other IIS pool with any .NET version (2 or 4) without conflicts with Service Connect Task Monitor.

2.7 .NET Extensions

The .NET extensions must be allowed for Service Connect to work correctly. After you install Service Connect, verify that .NET extensions are allowed. To do this:

1. From the **Start** menu, select **Run**. The **Run** window displays.
2. In the **Open** field, enter **inetmgr**. Click **OK**.
3. The Internet Information Services (IIS) Manager window displays. In the middle pane, double-click **ISAPI and CGI Restrictions**.
4. On the **ISAPI and CGI Restrictions** page, for each .NET extension, set the **Restriction** to **Allowed**.

2.8 SharePoint Component

If you are going to use SharePoint with Service Connect, you need to perform the following steps to install SharePoint component:

1. Copy the SharePoint install folder to the SharePoint server.
2. On the SharePoint server, in the appropriate bit folder, run SharePoint Integration setup (SharePointIntegrationSetup.msi).
Make sure, that the server name and port are valid.
3. Navigate to the `../windows/system32/drivers/etc` folder.
4. Open the **hosts** file in a text editor and add the following line: `<ESC_server_IP_address> scshost`.
For example: `192.168.0.123 scshost`

For detailed instructions on how to set up SharePoint Workflow refer to ESC online help.

3 Implementation

This part of the guide describes Epicor Service Connect implementation concepts and processes.

3.1 Concepts

Review the following section to learn about the main concepts of the Epicor Service Connect implementation.

Business Documents

Business document is a document containing business data. Epicor Service Connect receives business documents and processes them using custom workflows. Processing documents may include generation of new documents and sending documents to specific external recipients. Epicor Service Connect is able to receive and send documents in any format, but it uses only XML documents internally. All input documents that have other format must be converted to one of the internal XML document types before further processing. If an output document is required to be non-XML, it can be also converted to any format. Epicor Service Connect provides default converters that can convert XML, CSV and Microsoft Excel files into internal XML documents. If you need to support other formats, you may create custom components that support specific interfaces, and use them for conversion.

Epicor Service Connect internal documents always consist of a part containing system data (**message envelope**) and a part containing business data.

Documents are sent and received using Communication Channels. Communication Channels enable document exchange between Service Connect and other systems using various types of communication protocols. When document is received by communication channel, it can be converted to one of the internal documents for further processing in workflows. System part of the document may contain information about sender system or component. Sender credentials together with document type are used to create a type of subscription – **Message Mapping**. Message mapping allows launching an appropriate workflow automatically, when the document of certain type sent by certain sender is received.

Workflows

Workflow defines a sequence of automatic actions and user-performed tasks for processing business documents. General actions, like document transformation or assigning tasks to user, are provided by Epicor Service Connect services. More business specific actions can be incorporated into workflow by importing web-services that provide required functionality. (See the **Import Web Services** section and **Epicor Service Connect Documentation Kit > Using Epicor Service Connect > System Administration > Connectivity > Configuring Epicor Service Connect to Use External Web Services** for more details)

Workflows are organized in packages. Packages provide a convenient way to group workflows. You can create packages in Administration Console and Workflow. Administration console also supports backup and restore operations for workflow packages and individual workflows.

3.2 Processes

This part of the guide describes the order and the processes you perform to implement Epicor Service Connect. Note that the processes described below do not include achieving agreements with data and service providers

regarding business documents exchange, communications protocols and business operations included into the workflow.

3.2.1 Register Documents

The document is considered registered if the system can access XML schema of the document. The schema that describes system part of the document is a part of the Epicor Service Connect, so you only need to specify the schema for business data.

The business document may be registered using three ways:

- **Import Web Service.** When importing web services, the documents used in document exchange between Service Connect and web-service are registered automatically. For more information, see the **Import Web Services** section.
- **Use schema export utility.** Schema export utility automatically creates a schema using sample files.
- **Copy XML schemas manually.** If you already have XML schemas describing XML documents you plan to use, you can copy them manually to the **<SC installation folder>\SCS\UserSchemas** folder.

3.2.2 Import Web Services

Importing web-services is done in the administration console (For more information, see **Epicor Service Connect Documentation Kit > Using Epicor Service Connect > System Administration > Connectivity > Configuring Epicor Service Connect to Use External Web Services**). Imported web services become available for using in workflows and automatically register business documents used in message exchange between web service and Epicor Service Connect.

3.2.3 Set Up Communication Channels

Communication channels are used for sending and receiving documents. You need to configure communication channels before using them. During communication channels configuration, you can specify the following settings:

- Communication protocol and protocol specific settings, for example folder path for File channel
- Message encoding and format
- Acknowledgment
- Channel schedule
- Default message attributes
- Conversions

For more information, see **Epicor Service Connect Documentation Kit > Using Epicor Service Connect**.

3.2.4 Create Workflows

At this stage you are ready to create workflows. Workflows are created and edited in the Workflow Designer tool. For more information, see **Epicor Service Connect Documentation Kit > Using Epicor Service Connect > Workflows > Managing Workflow Processes in Workflow Designer**.

3.2.5 Set Up Message Map

Message map is a type of subscription workflow to certain business documents sent by certain senders. During message map configuration, when a certain business document sent by a certain user arrives to the channel and passes necessary conversions, an appropriate workflow is automatically launched. For more information, see **Epicor Service Connect Documentation Kit**.



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>.