Kinetic Architecture Guide

Version 2023.2

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.

Table of Contents

Getting Started 6

Hardware Requirements 7

- Configuration #1: One Server 7
- Configuration #2: Two Servers 8
- Configuration #3: Three Servers 8
- Configuration #4: Four or More Servers 9

Kinetic Components 11

- Administration Console 12
- Kinetic Server 12
- Application Server 12
- Database Server 13
- Kinetic Database 13
- Reporting Server 13
- System Agent and Task Agent 14

Extension Components 16

- Enterprise Search 16
- Information Worker 16
- Data Discovery 16
- Classic Web Access 17
- Classic Mobile Access 17
- Classic Education 17
- Classic Help 18
- Custom Configurator 18

Supplemental Components 20

- Collaborate 20
- Country Specific Functionality (CSF) 20
- Microsoft Service Bus 1.1 20

Cross-Brand Products 22

- Advanced Financial Reporting 23
- Epicor Commerce Connect 23
- Enterprise Performance Management 24
- Epicor Financial Planner 24
- Data Collection 24
- Epicor Shipping 25
- Service Connect 25
- XL Connect 25

Epicor Data Analytics ... 26
Utilities and Resources ... 27
Performance and Diagnostic Tool ... 27
Data Management Tool ... 27
Multiple Application Servers ... 29
Web Farm / Web Garden Notification ... 29
Customization Storage ... 30
Authentication Modes ... 32
Endpoint Binding Matching Modes ... 32
Basic Authentication ... 33
Windows Authentication ... 33
Azure AD Authentication ... 33
IdP Authentication ... 33
Example URLs Between Previous Versions and Kinetic 2022.1 ... 34
Configuration Changes ... 35
WCF Service Support ... 36
Authentication Options ... 37
Windows Account ... 37
Kinetic Account ... 37
Azure AD Identity ... 38
Epicor Identity Provider ... 38
Security Requirements ... 39
Licensing ... 39
User Account Options ... 39
Server Protection ... 39
Securing Database Access ... 40
Using the Windows Domain Account ... 40
Encrypting the Host.config File ... 40
SSL: Review Digital Certificates for Kinetic ... 41
Timeout Settings ... 43
Adjusting Timeout Settings ... 43
SSRS Site Timeout ... 44
Minimum Number of Threads ... 45
Trace Flags ... 47
Activating Trace Flags ... 47
Epicor Administration Console ... 47
The Server Log ... 48

Trace Flags List 49
Managing Telemetry 63

Getting Started

Welcome to the Kinetic Application Architecture Guide. This comprehensive guide provides a detailed overview on the supported technology and architecture of the Kinetic application.

Hardware Requirements

In this article, you can view hardware requirements for Kinetic. You can review the documents provided for hardware sizing and configuration, and you can also review example hardware configuration scenarios based on your required applications. It is highly recommended that you understand your hardware requirements prior to installing Kinetic.

Log on to EPICweb and go to the customer portal website and use the Search field to locate the **Kinetic Hardware Sizing and Configuration Guide**. Note that Hardware requirements may change based on the specific release. It is recommended that you have an understanding of the hardware requirements prior to installing. Use the guide to identify your hardware requirements.

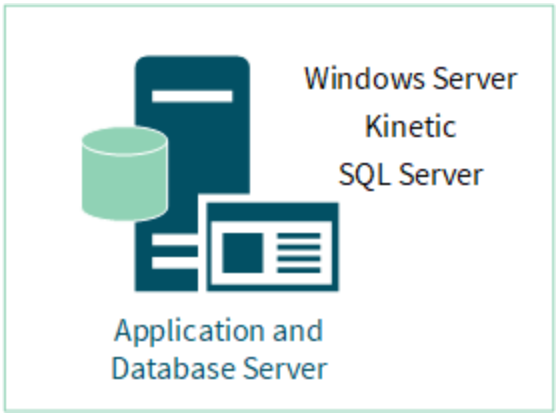
Below we cover the examples of hardware configuration scenarios, including basic multi-server scenarios. The examples list the applications that might be installed on each server. Review the example scenarios to determine which type of configuration is appropriate for your environment. Note that these are basic examples and your desired configuration may be more complex.

The example scenarios only use compatible versions of Windows Server and SQL Server:

- Windows Server 2016 with SQL Server 2017
- Windows Server 2019 with SQL Server 2017 or 2019
- Windows Server 2022 with SQL Server 2019 or 2022

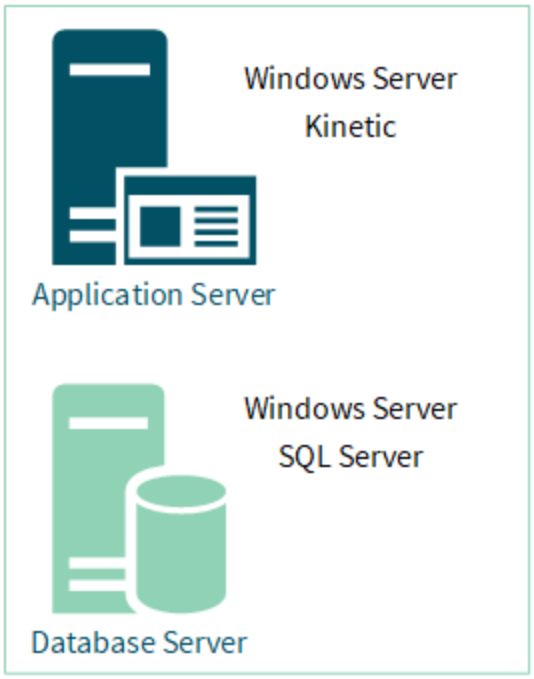
Configuration #1: One Server

Review the One Server configuration example to determine if it is appropriate for your environment.



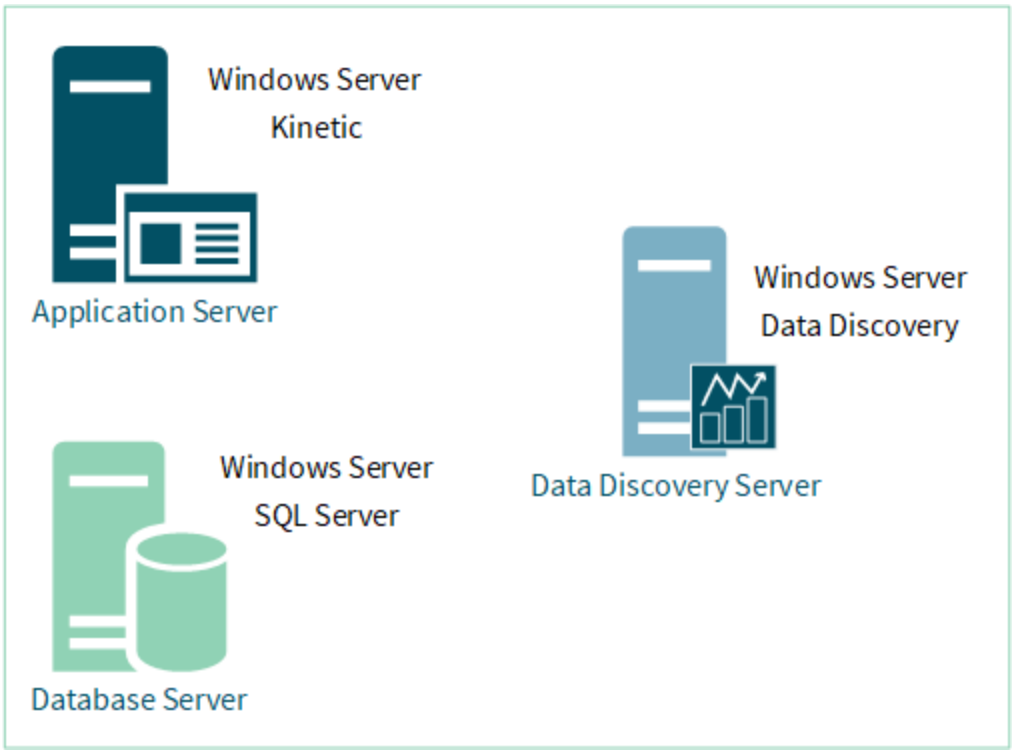
Configuration #2: Two Servers

Review the Two Servers configuration example to determine if it is appropriate for your environment.



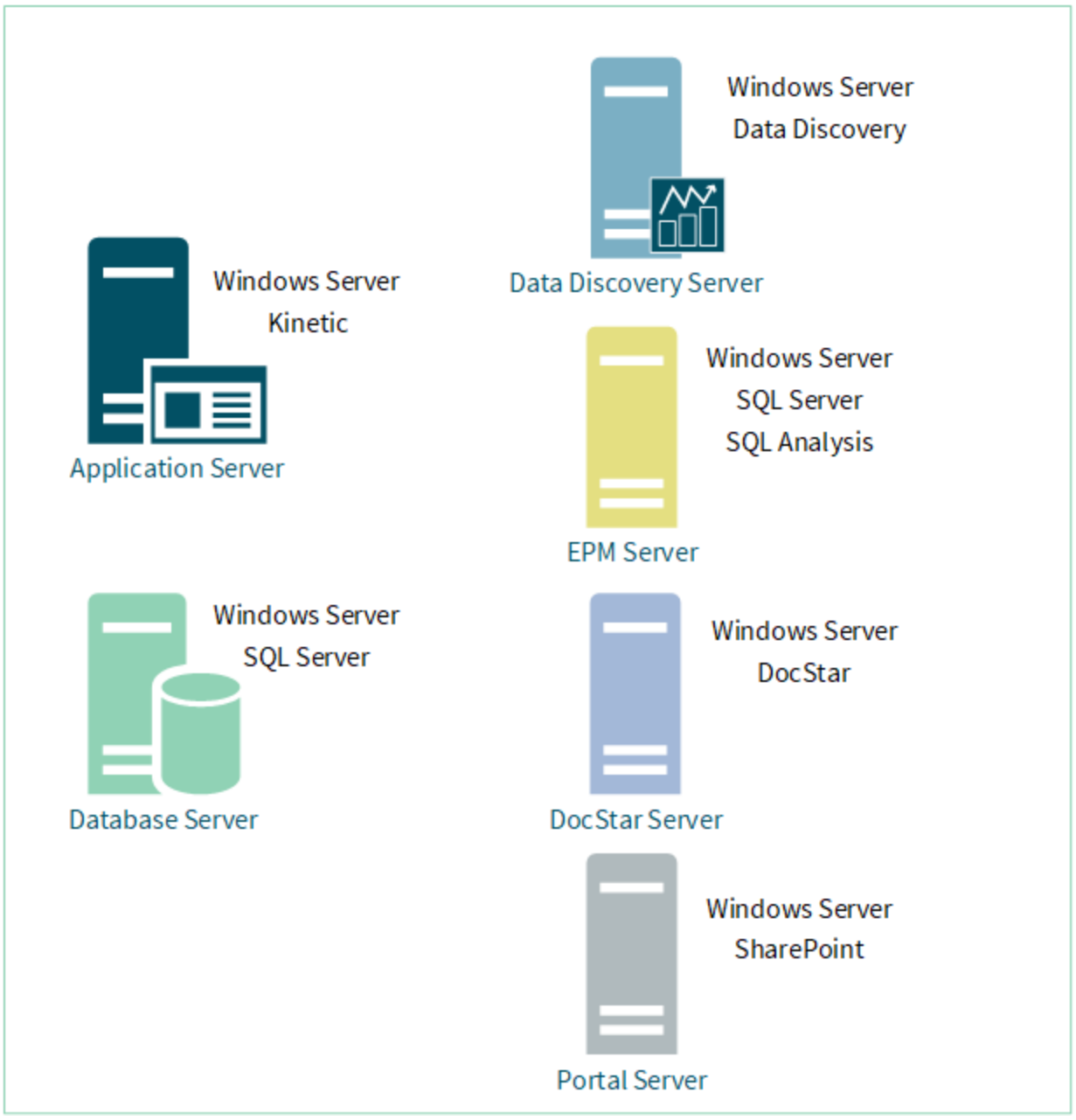
Configuration #3: Three Servers

Review the Three Servers configuration example to determine if it is appropriate for your environment.



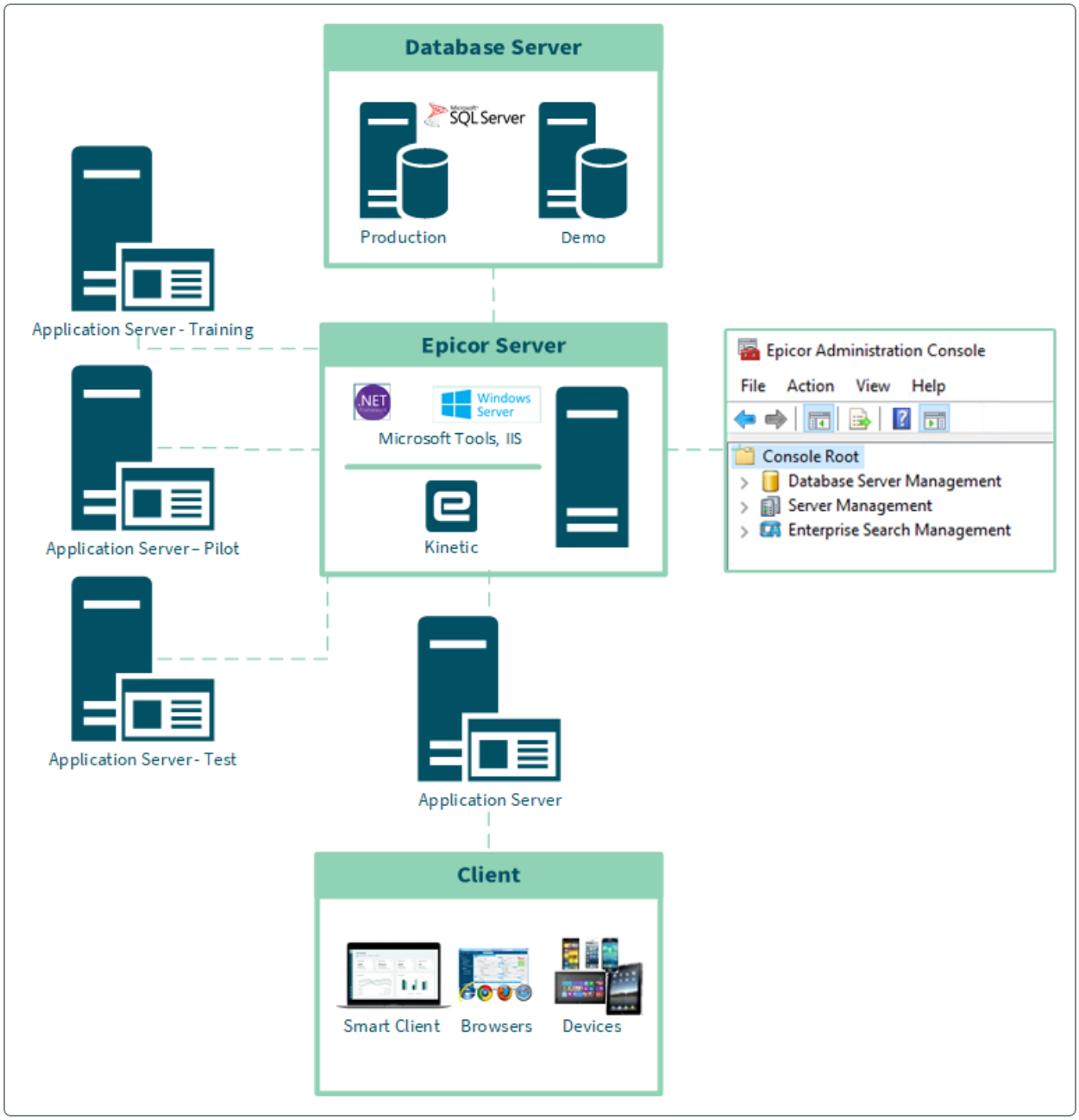
Configuration #4: Four or More Servers

Review the Four or More Servers configuration example to determine if it is appropriate for your environment.


Windows Server
Data Discovery
Data Discovery Server
Windows Server
Kinetic
Application Server
Windows Server
SQL Server
SQL Analysis
EPM Server
Windows Server
SQL Server
Database Server
Windows Server
DocStar
DocStar Server
Windows Server
SharePoint
Portal Server

Kinetic Components

Use this section to review the components of Kinetic. We recommend that you understand the relationships between the required components prior to starting your Kinetic application installation.



Administration Console

The Administration Console includes administrative tools that you can use to maintain and manage your application databases, application servers, Enterprise Search servers, and other system components. Using the Administration Console, you can manage multiple Kinetic server installations on multiple physical servers from a single interface.

Note that during the Development phase of a new release, we executed a range of QA cycles while using Kinetic application databases encrypted with SQL Transparent Data Encryption (TDE). No functional or performance issues related to running Kinetic on a TDE-encrypted database were seen. TDE is a technology used by Microsoft Corporation to encrypt SQL Server, Azure SQL Database, and Azure SQL Data Warehouse data files, known as encrypting data at rest. For more information on TDE, refer to the Microsoft documentation and articles. For example: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption.

Kinetic Server

Kinetic server is a server computer that hosts one or more Kinetic application servers. To define what application servers each Kinetic server hosts, you either create new application servers or register existing application servers. These application servers are then linked to the Kinetic server and run tasks for the Kinetic application.

Application Server

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

An application server is created under the Kinetic server. One or more application servers can be defined for each Kinetic server. When you select an application server on the tree view, you can perform administrative tasks to it. For more information on Kinetic server, review the Kinetic Server section within this guide and the Administration Console Help.

You can set up multiple application servers to run the same database. They can then improve performance by balancing the load. For example, you create two application servers for the same database, but these application servers support different endpoint bindings. One application server is set up to run to run a smart client through http on one server machine, while another application server is set up to run a smart client through https on a different server machine. For more information on Endpoint Bindings, review the Authentication Options section within this guide.

Database Server

A database server represents a SQL Server server\instance and contains the various Kinetic application databases your organization requires to conduct business. Before you can work with databases in the Administration Console, you need to add a database server to the Database Server Management node.

Kinetic Database

The Kinetic Database resides on the Kinetic Database Server.

For implementation following the Epicor Signature methodology you need four databases. Below are suggested names for the types:

- Kinetic_Demo - contains Demonstration Data. You can use it for Epicor University training and when you use the Hands-On courses or the Classic Education module.
- Kinetic_Test - includes your data. You can use it for test and development purposes and to try new scenarios.
- Kinetic_Pilot - contains your data for the Pilot database. The data should be controlled more than the Test database.
- Kinetic_Production - contains data you use to leverage various processes in your company.

Reporting Server

Reporting Server contains SQL Server Reporting Service (SSRS), a server-based reporting platform that provides comprehensive reporting functionality for a variety of data sources. Note that in Kinetic, SSRS reports can be used in parallel to Crystal reports.

Either install SQL Server Reporting Services (SSRS) 2017 with SQL Server 2017, SSRS 2019 with SQL Server 2019, or SSRS 2022 with SQL Server 2022. You must use Native Mode to print standard Kinetic reports.

If you have an existing Epicor 9.05 application and you chose to not use the recommended SSRS functionality that is available with Kinetic, you can use the steps in the Kinetic Migration Guide to install and configure SQL Server Reporting Service (SSRS) using the previous method, referred to as the "portal method". These steps will create the SSRS Portal, create the SQL Report Monitor Service, and establish the connection to a SQL Report Server. This portal method is available to provide a "stop gap" functionality that you can use to continue to have reporting functionality as you gain experience using the new SSRS functionality available in Kinetic.

System Agent and Task Agent

System Agent and Task Agent are designed to streamline and automate the flow of data throughout your company.

To maximize the efficiency of your network resources, you can select to execute reports, process programs and run queries not right after you submit them, but at a later time by adding them to a schedule that occurs during specific intervals. You can add programs to recurring schedules using the Schedule drop-down lists available on programs throughout the Kinetic application. When you assign a task to a recurring schedule, the Task Agent activates and handles it according to the settings defined by the System Agent. Review the following information to learn more about System Agents and Task Agents.

Any process, report, or other function defined as a startup task runs when the task agent starts. Because they use a startup task schedule, they do not use a Next Run On time value to launch. If a start up task is interrupted, it will run when the task agent is stopped and restarted.

- **Creating a System Agent**. A System Agent defines the information needed to configure the Task Agent AppServers. You create it after you first install the application, and it is automatically created when you install a Demo Database or migrate from a previous version. You then can use the System Agent > Detail sheet within the System Management Maintenance program to make changes you need to the system agent.

  Review Kinetic Installation Guide for information on how to set up System Agent. For more information on how to work with System Agent, review the Application Help.

- **System Agent Maintenance**. You use System Agent Maintenance to define schedules users can then select on reports, processes, and executive queries. Each schedule is set up to activate at regular, specific intervals - seconds, minutes, days, weeks, and months. When the system clock activates a schedule, all the tasks assigned to this schedule run. Depending on the task, this could cause a specific report to generate and print, a business activity query to export, a global alert to be sent, and so on. If a task generates an error and does not complete its process, the other tasks on the schedule will continue to run as expected.

  Then to make better use of your system resources, you can also create task agent rules. These task agent rules divide the system agent's processing between different application servers. An application server manages how a specific instance of the Kinetic application runs. You can set up multiple application servers to run the same database and balance the load. You could create

two application servers for the same database, but these application servers are linked to different server machines.

To run the Task Agent, you must configure your System Agent Kinetic user account to have session impersonation rights. For instructions on how to set session impersonation rights, refer to the Kinetic Installation Guide.

- **Task Agent Service Configuration**. You can create a task agent in the Task Agent Service Configuration program. This program allows you 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. If you have multiple appservers, all of them point to the same database, and you can configure a task agent on any appserver even if they are located on different physical servers. The task agent is distributed to multiple appservers based on pre-defined rules. You can set up a maximum of three task agents to run against the same database.

- **Connecting a Task Agent**. You can connect a task agent to an application server through different endpoint binding methods. If you 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 a Kinetic or ICE user account.

Review the **Authentication Options** article for more details on the binding methods you can use in Kinetic.

Extension Components

You can install the extension applications after you have configured your Kinetic application server.

To get an extension working, you need to go through the following three-step process:

- Select the extension features to install during the Kinetic server installation process.
- Deploy the selected features, use the Application Server Configuration process in Epicor Administration Console.
- Perform initial configuration within the installed extension.

Enterprise Search

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

Using the default search index definition shipped with Kinetic, you can search on any item within the Kinetic database - like a part, customer, purchase order, AR invoice, and so on. All the records within the Kinetic 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.

Information Worker

Information Worker is a set of plug-in applications for Microsoft Office that offers a transparent user experience for Kinetic applications within a familiar desktop productivity environment. It gives employees who depend on enterprise data ("information workers") direct access to Kinetic data from inside Microsoft Outlook, Word and Excel.

Once Kinetic data is imported into Office, users can keep the data synchronized between Office and Kinetic, and can work either in online or offline (disconnected) modes.

Data Discovery

Data Discovery (EDD) is a Business Intelligence solution intended to provide an extremely easy to use sense-making, data exploration, data visualization experience. EDD is a major component of the overall

data platform which encompasses a broad set of capabilities for managing, accessing, sharing, cleansing, visualizing, and extracting insights from data created by or related to Kinetic created data

Classic Web Access

Classic Web Access (formerly Epicor Web Access or EWA) displays Epicor Commerce Connect (ECC) forms. Through this site, you can quickly find the ECC applications you frequently use. This site can run on several operating systems and on a variety of devices - including handheld devices. If you have an EWA site for a previous release, running the **Reinstall** function will update the site to only display ECC forms.

Previously EWA displayed the Kinetic smart client Classic applications in a browser, but these forms are no longer available. If you reinstall and then deploy this EWA version, you will lose access to ALL Kinetic applications. If you attempt to display them, you will get a server error.

If you want to use a browser for working with Kinetic UX applications, either continue to use the previous EWA version or switch to the Home Page in the browser client. For information on how to use this interface, refer to the **Using Kinetic Applications in Smart Clients and Web Browsers** article in Help and Support Center.

Classic Mobile Access

Classic Mobile Access (formerly Epicor Mobile Access or EMA) extends the Epicor Everywhere Framework™ to generate properly sized Web forms for mobile platforms including iPhone, Android, and Windows Phone.

Since the mobile dashboards that support Classic Mobile Access are built using the dashboard technology and Updatable BAQ technology embedded in Kinetic, users can create web applications that implement business functionality on mobile devices.

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

Classic Education

The Classic library of embedded educational materials provides you with a platform to develop 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.

If you want to install the Classic Education module for use with your desktop client, contact Epicor Support and request this module file. Epicor will send you this file using File Transfer Protocol (FTP).

After you install the module file, you can launch the education courses by using the Classic interface and clicking Help > Education.

Starting with Kinetic 2021.1, we are putting Embedded Education for Classic into Maintenance Mode. The Embedded Education link is removed from the Help and Support Center panel to provide a single point of access to all education materials - Epicor Leaning Center.

New Hands-On Exercises are available for Kinetic UX applications. This is the next generation of workshop-based courses for use with the application. These courses are available on Epicor Learning Center (ELC) as part of learning agendas. Agendas can contain Training on Demand (TOD) videos topped off with a true in-app experience provided by Hands-On Exercises. You can access education agendas from ELC (Quick Views> Agendas).

Classic Help

Classic help system contains reference level information on modules and programs of the Classic progam UIs. It also contains a series of technical references guides that provide detailed information on job costing, scheduling, and other areas of the Kinetic application.

If you want to install the Classic Help to use with your desktop client, contact Epicor Support and request this file. Epicor will send you this file using File Transfer Protocol (FTP).

After you install this file, you can launch application help from the Classic Home page by clicking the Help tile, or from directly within a specific program by pressing the F1 key or clicking Help > Application Help.

Classic Help extensions displays information for the Classic programs only and its help no longer appear in the search results in Help and Support Center on the Kinetic Home Page. If you install this extension, you can still access Classic help via the Classic application window.

Custom Configurator

Custom Configurator (formerly Epicor Web Configurator or EWC) is a web-based client for the Configurator you can use to work with the Epicor Commerce Connect Dealer Portal that links

manufacturers directly with dealers. This functionality is designed for manufacturers who sell configured products through a distributor or dealer channel. By receiving transactions from dealers through the Dealer Portal, these manufacturers can sell their products, track products after they ship them, and support warranty and repair needs.

Supplemental Components

Supplemental components that can be installed after your Kinetic application is installed and configured.

Collaborate

Collaborate is a cloud-based solution that simplifies collaboration, drives employee engagement, and streamlines interaction processes by leveraging social media concepts like hashtags and mentions. Collaborate enables different teams to work together around orders, customers, suppliers, configurations, projects, or any other business objects within Kinetic; bring sales and manufacturing together, share, comment, and move on.

You can easily track information about an order as it progresses from a lead all the way until payment is received in a dedicated stream available within your Home Page and Quick Access panel. This means your activity stream shows you what you need to know, when you need it, exactly where you need to see it in order to do your job effectively.

For more information about Collaborate, refer to the articles in Help and Support Center.

Country Specific Functionality (CSF)

Country Specific Functionality is designed to accommodate localization for specific markets throughout the world. It supports global, regional and local accounting and reporting standards such as, IFRS, Generally Accepted Accounting Principles (GAAP), taxes and fiscal reporting Support for various countries.

You can view the list of available countries in the Kinetic Installation Guide and activate the required country in Epicor Administration Console.

Microsoft Service Bus 1.1

Microsoft Service Bus for Windows Server, also called "Service Bus", is required as a software component with Kinetic if you use Multi-Company functionality and you process multi-company transactions between more than one database. Using queue technology, Service Bus provides extensive publish/subscribe capabilities which allow multiple, concurrent subscribers to retrieve views of the published message stream.

Review the Service Bus prerequisites when installed for use with Kinetic:

- Windows Server 2016, Windows Server 2019, Windows Server 2022
- SQL Server 2017 or 2019
- .NET Framework 4.8
- TCP/IP connections or named pipes configured in SQL Server
- SQL Browser service running in case of TCP/IP connections.

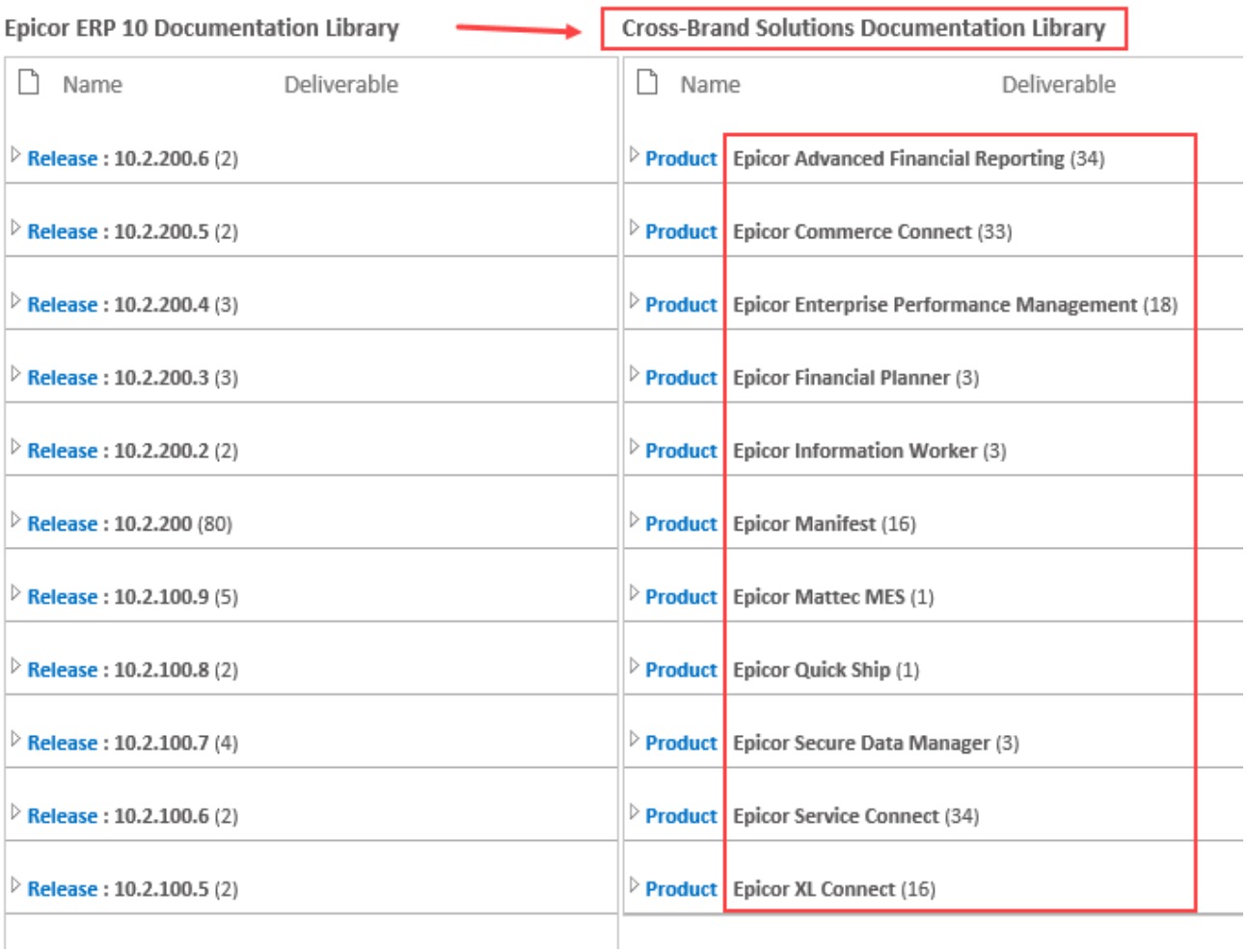
SQL Server can be installed on the same physical machine with the Service Bus or on a different machine. The Service Bus databases can reside on multiple machines as well. All the databases do not need to be created on a single database server.

The instructions for installing Microsoft Service Bus for Windows Server are located in the Kinetic Installation Guide (New or Migration) > Supplemental Installations section. For additional information, you can also refer to the Microsoft Download Center documentation. Note that the instructions for setting up Multi-Company functionality is located in the Multi-Site Technical Reference Guide which is available within the online help.

Cross-Brand Products

Use this section to review the Cross Brand Products that can be installed after you install and configure Kinetic.

You can access the Epicor Cross-Brand Solutions documentation on EpicWeb using the following link:https://epicweb.epicor.com/products/kinetic-erp/documentation/on-premises. The Cross-Brand Solutions library is in the right pane. Your screen may look similar to the following:



Epicor Cross-Brand Solutions are designed to extend the functionality of Kinetic by providing additional features you can use for your business requirements. You can configure these products to work with different ERP systems, such as Kinetic, Prophet 21, iScala. Eclipse, Tropos and so on. Cross-Brand solutions interact with your ERP system which allows you to use ERP data in additional environments.

Advanced Financial Reporting

Epicor Advanced Financial Reporting is a complete toolset you use to create custom financial reports specific to the needs of your organization. The reports you build will contain financial information from various sources you define - you can set up each report to pull information from one or multiple general ledger (GL) books across multiple companies, from multiple ERP systems.

Epicor Advanced Financial Reporting interacts with an Kinetic application through a report server. This server pulls the general ledger data from your active database to an AFR financial database via replication provided by AFR Replication Monitor, and makes this data available for use within AFR. You then create a report definition in the Report Designer.

The AFR Report Designer is used to define the basic elements of the reports - row sets, column sets, report parameters, data filters, and formatting of the reports. Using the Report Designer, you can build report definitions, preview them to verify current data displays as expected, and upload Report Definition Language (RDL) files, which enable users to view reports in a web browser, via SQL Server Reporting Services (SSRS). Once you set up your report, you can further refine the look and feel in either Microsoft® Visual Studio® or Microsoft® SQL Server® Report Builder. You can use these report layout and formatting tools to fine-tune the overall look of each financial report.

When you finish refining the layout of your financial reports, users can view them in a web browser or in Microsoft®Excel®. Reports can be printed, or exported in various file formats, or you can schedule a batch of reports to be created at regular intervals. Based on the report parameters you define in the report, users can filter data, or change the parameters to view different data, for example, change the report currency, change the report dates, or filter by GL accounts.

AFR is not compliant with the FIPS 140-2 cryptography standard.

Epicor Commerce Connect

Epicor Commerce Connect is an e-commerce solution that enables Kinetic customers to develop unique websites quickly and manage them easily, providing the necessary tools to deliver a rich customer experience, throughout the typical order life cycle - from quote to fulfillment, and beyond.

Fully integrated to your ERP system, Epicor Commerce Connect eliminates the need to maintain a separate product database and provides streamlined access to ordering, product or account information including customer specific pricing, inventory levels, marketing and customer service processes - all in real-time using ERP data that can be viewed online via Epicor Commerce Connect.

Based on the Magento eCommerce platform, Epicor Commerce Connect provides a scalable solution that is backed by an extensive support network and allows you to build a site to help fit your unique business needs.

Epicor Commerce Connect is not compliant with the FIPS 140-2 cryptography standard.

Enterprise Performance Management

Epicor Enterprise Performance Management (EPM) provides a complete set of tools and applications that let you plan, execute, and analyze at both strategic and tactical levels – aligning business activities with business goals. A business support system, EPM supports the complex analysis required to discover business trends. The information retrieved from this analysis is valuable in identifying trends and modeling data in the areas of planning, budgeting, forecasting, financial reporting, and data warehouse reporting.

EPM solutions integrate monitoring and analysis with the planning and control (or audit) cycle of the enterprise to enable a cycle of continuous performance improvement.

EPM is not compliant with FIPS 140-2 cryptography standard.

Epicor Financial Planner

Epicor Financial Planner (EFP) provides functionality to automate the financial planning and budgeting process to keep your records accurate and up-to-date. It provides a complete system for financial budgeting and forecasting. Epicor Financial Planner allows Kinetic customers to improve automation and take control of the budgeting and planning process, allowing you to rest easier with more certainty in your projections.

Data Collection

Data Collection is a real-time production and process monitoring system which can be used as a powerful tool in manufacturing including rubber and plastics, metals and automotive industries.

The solution offers a comprehensive set of Data Collection capabilities for production scheduling, machine operation and maintenance, quality management, and real-time analytics to monitor machines and analyze machine-related data such as overall equipment effectiveness (OEE), run rates, scrap, yield and energy consumption. The system captures data directly from machines and operators, and delivers real-time production metrics and real-time operations analytics in an easy-to-digest visual manner.

Real-time reconciliation of information between Kinetic and Data Collection ensures data integrity for supporting accurate scheduling, planning, monitoring, resourcing and costing.

Use Data Integration to manage production from a central location and seamlessly integrate data flow between Kinetic and Data Collection. This integration allows you to reduce errors from manual data entry in both applications and get timely and accurate data to enable better manufacturing decisions. Kinetic production planning and job data are exported to Data Collection for use when performing and monitoring shop floor activities. In Data Collection, production data is monitored and recorded for use in process and quality control monitoring and analysis.

Labor and production data recorded in Data Collection will then flow back to Kinetic where the data can be used for costing, reporting and production analysis.

Data Collection is not compliant with the FIPS 140-2 cryptography standard.

Epicor Shipping

Epicor Shipping (formerly known as Quick Ship) bridges the gap between Kinetic and your parcel carrier for domestic parcel shipments. Epicor Shipping uses FedEx and UPS web services to get your shipments out faster and easier. Epicor Shipping imports all of the data — including shipping and packaging codes—directly from Kinetic using REST Services.

Service Connect

Service Connect is a workflow and application integration environment. You can use Service Connect to run a workflow within a single application or to run workflows that span multiple applications. Because it uses documents as its primary interface and leverages a Service Oriented Architecture (SOA), Service Connect simplifies the data conversion process from one application to suit the needs of other applications.

Service Connect is not compliant with the FIPS 140-2 cryptography standard.

XL Connect

XL Connect is a powerful tool that can be used to report on data currently stored in your accounting system. XL Connect is an add-in to Microsoft Excel™ and is accessed from within Excel. XL Connect is the data retrieval engine. When in Excel, you will use XL Connect Content Functions and Analysis Sets to build reports that will retrieve your accounting system data.

XL Connect Content provides the integration specific elements that define for XL Connect the tables in your accounting system from which to retrieve your requested data. Once the data is retrieved into

Excel, you can use all of Excel's capabilities to create a report that meets your business needs: financial statements, budget reports, sales analysis, invoice analysis and dashboards.

XL Connect is not compliant with the FIPS 140-2 cryptography standard.

Epicor Data Analytics

Epicor Data Analytics provides interactive dashboards and analysis of the data inside your business system. The dashboards provide visual displays, so you quickly see important information about how your business is performing. Unlike a spreadsheet, you can "drill down" into the data by clicking on it to see the details that you need for the task at hand.

Utilities and Resources

Use this section to review the utilities and resources that are available and can be used with Kinetic .

Performance and Diagnostic Tool

You can use the Performance and Diagnostic Tool (PDT) to analyze Kinetic logs to measure performance from both the client and the server. PDT summarizes information in the client and server trace logs. You can manipulate that information to provide meaningful metrics related to the installation efficiency and performance of Kinetic .

Performance and Diagnostic Tool offers the following utilities:

- **Client Diagnostics**- use it to analyze the performance of client installations.
- **Configuration Check**- use it to check the configuration of the application server. This utility reveals the issues and potential issues you may have with the application server configuration.
- **Network Diagnostics**- use it to verify the baseline network and server performance are running at optimal levels.
- **Server Diagnostics**- use it to analyze the performance of server installations.

The Performance and Diagnostic Tool is run from the Epicor Administration Console. For information on how to run PDT, use the Performance Tuning Guide.

Data Management Tool

You can use Data Management Tool (DMT) to accelerate and simplify the data migration process as well as efficiently maintain your existing system data.

DMT offers the following features:

- Improve your implementation timeline and migration process.
- Import, add, update, and delete application data safely and efficiently.
- Application logic ensures security, data integrity and optimal performance.
- Imports data from commonly used Microsoft Excel and .CSV files.

- Provides estimate of the time it will take to import data.
- Error log identifies specific import problems.

DMT is delivered as additional files to be placed in the Kinetic client directory.

Multiple Application Servers

If you have a multiple application server environment, use this section to review information specific to web farm and web garden configurations.

Web Farm / Web Garden Notification

When multiple application servers are connected to the same database, each can internally notify all application servers in the web farm or web garden that a change occurred. The application servers in this web farm or web garden then refresh with the required changes.

This feature is useful for web farm, web garden, or other multiple application server environments. For example, when the database changes or a BPM assembly is updated, the application server with the change sends out an internal notification. If this update is a database change, the application servers refresh their caches. If this update is a BPM assembly change, the application servers regenerate their BPM assemblies.

You can set up these notifications by selecting the notification type that best reflects your network configuration. To do this, modify the **host.config** file for your environment. This file is located in your server installation. For example: C:\Epicor\ERP11\11.2.300.0

Set up the **NotificationType** to define how the application servers send notifications to the group. The available notification types are:

- **local** - Select this option to indicate a single application server is in this web farm / web garden and no internal notifications are needed. Always select this option when only one application server is in the web farm / web garden, as it improves performance by reducing unnecessary notifications.
- **UDP** - Indicates the notifications are delivered through a User Datagram Protocol (UDP) broadcast. This protocol exchanges messages between all computers in a local area network (LAN). This notification type does not work on a wide area network (WAN). If your application servers are on the same LAN and the required ports are open, a UDP broadcast can reach them. You should then select this option.

  For the **NotificationUdpPort** setting, be sure to enter a unique and unused port for each application server group. This requirement ensures the internal notifications are only sent within a specific application server group.
- **database** - Select this option when you cannot use the UDP option and you are running more than one process or application server. Depending on how your network is configured, you may

not be able to select UDP and so you instead must send notifications through the database. While this option is the most reliable, this setting increases the number of calls to the database and so reduces performance. If your environment supports UDP, you should use the UDP option instead. Note that the default type is database.

Use these steps if you need to change the type to the one that best reflects your network configuration.

1. Navigate to your application server **host.config** file. This file is located in your server installation, for example, Epicor\ERP11\11.2.300.0.
2. Locate the **NotificationType** entry.
3. Set the value to one of the options.

   If you set the notification type value to **UDP**, you also need to specify the **NotificationUdpPort** property which defines the unique port used by the application server group.

   Your file may look similar to the following:

   ```
   <!-- Valid values: local, UDP or database -->
   <add key="NotificationType" value="UDP" />
   <!-- Valid values: 1024-65535. Choose a different port for each
   group of AppServers -->
   <add key="NotificationUdpPort" value="3100" />
   ```

4. Save and close the host.config file.

Customization Storage

For multiple appservers scenario, we recommend to use a shared location to distribute active customizations and their dependencies between multiple environments.

Customers hosting several endpoints, those running the web farm or web garden may set up the web.config as follows:

- Customization storage provider (customizationStorage - provider attribute) configured to use SqlBlob. This option is set by default.
- Storage of external assemblies (externalsStorage - providerattribute) configured as FileSystem, pointing (externalsStorage - settingsattribute) to a single shared folder location for all instances in the web farm/web garden corresponding to a single installation. When setting up access rights

to the folder, make sure that Application Pools of all participating web applications have at least read access.

Example: Use DFS or UNC (common) path -\\server\share\folder accessible to all appservers.

```
<customizationSettings disabled="false" intermediateFolder="                                    ">
  <customizationStorage provider="SqlBlob" />
  <externalsStorage provider="FileSystem" settings="\\centralServer\ShareForE10\Install1\ExternalAssemblies" />
```

Authentication Modes

Starting with Kinetic2022.1, the server was upgraded from .NET Framework 4.8 to .NET 6. Kineticsmart clients still use .NET Framework 4.8. While Microsoft will continue to support the .NET Framework, .NET 6 is the next version of this technology. Designed for the cloud, .NET is a scalable platform with regular updates.

This simplifies how you set up application servers and task agents. Instead of using several types of endpoint bindings, the system now uses authentication modes. These modes determine how the system authenticates users. This also replaces WCF with Web APIs, leveraging the benefits of the cloud architecture.

Authentication modes always use HTTPS, ensuring better security for your system. You can also enable HTTP, but this is disabled by default. The modes DO NOT use NET.TCP, as NET.TCP is deprecated in the system.

The available authentication modes are **Basic**, **Windows**, **AzureAD**, and **IdP**. This topic details how you move from endpoint bindings to authentication modes. It also describes each mode and when you use it on your task agent or application server.

Endpoint Binding Matching Modes

This table shows the previous Endpoint Bindings and their matching .NET 6 Authentication Modes.

Kinetic2021 Endpoint Binding	Kinetic2022 Authentication Mode
HttpsBinaryAzureChannel HttpsOffloadBinaryAzureChannel	AzureAD
HttpsBinaryIdpChannel HttpsOffloadBinaryIdpChannel	IdentityProvider
TcpBinaryUsernameSslChannel UsernameWindowsChannel HttpsBinaryUsernameChannel HttpsOffloadBinaryUserNameChannel TcpBinaryUsernameWindowsChannel HttpBinaryUsernameSslChannel UsernameSslChannel	Basic

Kinetic2021 Endpoint Binding	Kinetic2022 Authentication Mode
Windows HttpsBinaryWindowsChannel TcpBinaryWindowsChannel	Windows

Different authentication modes do not require a secondary or integration AppServer. This makes it easier for users to log into the client.

Previous Kinetic versions defaulted to an XML response, but now most endpoints return JSON. The exception is when a request asks for XML and does not include a JSON option. This includes the https://servername/appservername/api/.configuration endpoint.

Basic Authentication

Authenticates users by checking their Kinetic login names and passwords. You create these accounts and manage passwords within User Account Security Maintenance.

Windows Authentication

Authenticates users by checking their Microsoft™ Windows™ account. They use these credentials to log into your overall network. These this mode, users can log in using single sign on (SSO).

Note that to use this method, you also must select the **Allow Windows Authentication** check box on the application server. Select this check box so that IIS can authenticate users through their Microsoft™ Windows™ account credentials.

Azure AD Authentication

Authenticates users by first signing them in through the Windows Azure Active Directory (AD). Azure AD then sends a secure response back to the client and the users gain access to Kinetic.

If you use Azure AD and the browser client, select the **Allow Azure AD Authentication** check box. This option directs browser clients to first sign in users through the Windows Azure Active Directory.

IdP Authentication

This global authentication service unifies identity and authentication mechanisms across various Epicor platforms. When you enable the Identity Provider (IdP) mode in your environment, you can select this

option.

Example URLs Between Previous Versions and Kinetic 2022.1

URL	Endpoint Binding	Authentication Mode
SOAP	https://<EpicorCustomer>/ ERP /BO/*.svc https://<EpicorCustomer>/ICE /BO/ *svc via text/xml; charset=utf-8	https://<EpicorCustomer>/wcf/ERP/ BO/*.svc https://<EpicorCustomer>/wcf/ICE/ BO/*svc via text/xml; charset=utf-8
WinForm - Sysconfig	https://<EpicorCustomer>/; HttpsBinaryUsernameChannel	https://<EpicorCustomer>/; Basic
WinForm - Sysconfig - IDP	https://<EpicorCustomer>/; HttpsBinaryIdpChannel	https://<EpicorCustomer>/; IdentityProvider
WinForm - Sysconfig - AAD	https://<EpicorCustomer>/; HttpsBinaryAzureChannel	https://<EpicorCustomer>/; AzureAD
Kinetic UX - Browser version of Kinetic - URL	https://<EpicorCustomer> /apps/erp/home/ or https://<EpicorCustomer>/home	https://<EpicorCustomer>/apps /erp/home/ or https://<EpicorCustomer>/home
DMT	Uses WinForms client sysconfig file	Uses WinForms client sysconfig file
DocStar/ECM	https://<EpicorCustomer>/	https://<EpicorCustomer>/

URL	Endpoint Binding	Authentication Mode
HCM (legacy versions only; the current HCM version uses REST)	https://<EpicorCustomer>/ERP/BO/EmpBasic.Svc https://<EpicorCustomer>/ERP/BO/Indirect.svc https://<EpicorCustomer>/ERP/BO/Labor.svc https://<EpicorCustomer>/ERP/BO/PRDeduct.svc https://<EpicorCustomer>/ERP/BO/PREmployee.svc	https://<EpicorCustomer>/wcf/ERP/BO/EmpBasic.Sv https://<EpicorCustomer>/wcf/ERP/BO/Indirect.sv https://<EpicorCustomer>/wcf/ERP/BO/Labor.sv https://<EpicorCustomer>/wcf/ERP/BO/PRDeduct.sv https://<EpicorCustomer>/wcf/ERP/BO/PREmployee.svc
IDP Setup - URLs	https://<EpicorCustomer>/<IDPID>/Apps/ERP/Home https://<EpicorCustomer>/<IDPID>/Apps/ERP/Home/silent-renew.html https://<EpicorCustomer>/<IDPID>/Apps/resthelp/	https://<EpicorCustomer>/<IDPID>/Apps/ERP/Home https://<EpicorCustomer>/<IDPID>/Apps/ERP/Home/silent-renew.html https://<EpicorCustomer>/<IDPID>/Apps/resthelp/
TaskAgent - URL	net.tcp:// <EpicorCustomer>/	https://<EpicorCustomer>
EMA	https://<EpicorCustomer>/<CustomerID>-EMA	https://<EpicorCustomer>/<CustomerID>-EMA
EDD	https://<EpicorCustomer>/<CustomerID>-EDD	https://<EpicorCustomer>/<CustomerID>-EDD

Configuration Changes

As part of the support for cloud, application user settings that were in the **web.config** file are now moved to the **host.config** file. The system still uses the web.config file, but it now only contains Internet Information Services (IIS) settings. Because an application server can now run without ISS, these two files reflect how the system now runs in the cloud.

The application user settings in the host.config files are the same as the settings in the web.config file.

WCF Service Support

Some WCF service support is available. It is disabled by default within on premise environments, but enabled within cloud (SaaS) environments. Only a few services still use WCF, but you can add more services if you need.

Eventually this backwards compatibility will be discontinued. Use of SOAP is also deprecated. We highly encourage that all systems use both REST and the authentication modes.

Authentication Options

In this section, we cover the identity methods used to authenticate a user account. These methods have both advantages and disadvantages, so select the method that works the best for your organization. You define your user identity method when you implement single sign on. For more information on Single Sign-on and Azure AD authentication, refer to the Kinetic Installation Guide > Appendix section.

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

Windows Account

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

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

Kinetic Account

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

Azure AD Identity

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

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

Epicor Identity Provider

Epicor Identity Provider (IdP) is an authentication service that unifies various identity and authentication mechanisms across Epicor products, ensuring secure and easy to use products. Epicor Identity Provider allows applications to authenticate users registered in the common user database. Epicor Identity Provider issues signed tokens, which contain claims with required information. These tokens can be validated using Epicor Identity Provider public key.

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

For more information on user identity methods, refer to Kinetic UX Configurator help.

Security Requirements

In this section, we cover security requirements for Kinetic.

Licensing

In Administration Console, you use the Licensing node to manage licensing for your product licenses for an application server.

Using the licensing node, you can import or delete licenses and view the license properties. Properties include information such as the installation name, expiration date, and data on companies, license modules, and country specific functionality included in the installation.

User Account Options

Review the types of user accounts that must be created in Kinetic.

- **SQL Server User**. You set up an SQL Server User so that you have a login account to access the Kinetic database.
- **IIS Application Pool**. You can choose to use the default application pool provided by IIS on install, or you can create your own application pool. An IIS worker process is a windows process (w3wp.exe) which runs Web applications, and is responsible for handling requests sent to a Web Server for a specific application pool. Application Pool is a way to create sections or compartments in a web server. It allows you to isolate applications running on the same server, thus a crash on a single application/website does not bring down the entire server.
- **Kinetic application**. Application users are managed under the application server Users node in the Epicor Administration Console.

Server Protection

Review this section for information on how to set up such server protection features as ports to use for connection on the servers and anti-viral scan configuration.

You should use the following ports for connection on the servers associated with Kinetic:

Client and Kinetic IIS Servers	Kinetic IIS Server	SQL Server
• 808 (https) • 443 (ssl)	• 80 (default IIS/Report Server) • 9010 (task agent service) • 8172 (we check this port during the creation of appservers; aka: webdeploy port) • 8098/9098 (Enterprise Search)	• 80 (IIS/Default Report Server) • 1433 (SQL)

When you configure anti-viral software, we recommend to exclude the following folders from real time scans:

Kinetic Client Server	Kinetic IIS Server	SQL Server
• The ERP11\client folder • Client cache (by default, c:\programdata\Epicor)	• The root IIS folder (by default, c:\inetpub) • The root ERP11 folder (by default, c:\epicor\erp11)	• All folders that contain the SQL db files (ldfs/mdfs)

Securing Database Access

Securing database access from the application server is an important aspect to consider when installing Kinetic. Several methods are available to secure access to each database: Use the Windows Domain Account and Encrypting the Web.config File

Using the Windows Domain Account

The Windows Domain account can be used to run the application server. It is recommended that you do not use the same account across multiple databases. Each database should have an unique account. For example, use MyDomain\KineticServiceAccount. To use this account, do the following:

- In SQL Server, grant access to the Windows User.
- In the host.config file, use Trusted Windows Connection for the database setting.
- In IIS Manager, under Advanced Settings, assign the app pool to the Windows User.

Encrypting the Host.config File

The application server host.config file includes important SQL Authentication credentials, such as the SQL user name and password. To help secure the integrity of the credentials, it is recommended that

you encrypt the host.config file. Several methods exist for encrypting the host.config file, including:

- DataProtectionConfigurationProvider
- RSAProtectedConfigurationProvider

To learn more about encrypting configuration files, use the following Microsoft Developer Network links:

- "Walkthrough" Encrypting Configuration Information Using Protected Configuration". Click this link to review a step-by-step example on encrypting parts of a configuration file: https://msdn.microsoft.com/en-us/library/dtkwfdky(v=vs.100).aspx.
- "ASP.NET IIS Registration Tool". Click this link to review instructions on how to use the ASP.NET IIS Registration Tool (aspnet_regiis.exe). Link: https://msdn.microsoft.com/en-us/library/vstudio/k6h9cz8h(v=vs.100).aspx. You can use these configuration options:
  - **-pe** option can be to encrypt a specified configuration section and can be used with modifiers.
  - **-pef** option encrypts the specified configuration section of the host.config file in the specified physical directory.

SSL: Review Digital Certificates for Kinetic

Digital certificates play a key role in securing the communications between callers and services in the Kinetic application and ICE 4.1 Framework.

When Kinetic is installed, the web services (SOAP) and REST services can be hosted automatically by the Kinetic web sites. The SOAP-based web services can be used for integrations from either non-.NET callers or from callers that do not have Epicor binaries available. REST services are used with Classic Web Access. Both of these protocols require encryption using digital certificates.

The SOAP messaging protocol is designated as deprecated and replaced by REST. It will continue to work for two more releases (2021.1 and 2021.2) to give you time to adapt and move to better alternatives. You should plan on switching your integrations to use REST endpoints or client proxies.

You can set up your machine to use the sample X509 certificates available with Kinetic. These certificates do not expire until 2039 and are meant to be used during your Kinetic implementation. You can also replace these sample certificates with certificates that you create on from your own trusted servers or delivered from a Third Party company such as VeriSign.

We do NOT recommend to use self-signed certificates for Kinetic Servers that host the production database as they do not assure high security. Please study the available options and obtain an SSL certificate form a trusted Certificate Authority.

A digital certificate is basically a pair of keys - one public and one private. The public key can only decrypt data which was encrypted using the private key and vice-versa. By keeping the private key truly private, client applications using the public key are assured they are communicating with a known service. The digital certificates are used to verify that the service is really who or what you believe it is. A digital certificate is signed using (usually) the public key of another digital certificate, the private key being held by a trusted party. These signatures form a "trust chain". At the top of the trust chain is a "root" certificate, which used its private key to basically sign itself.

For commercial web sites, the trust chain follows one of a small number of primary certificate authorities. The images below show the trust chain for a bank's website. You can see this chain by clicking the padlock icon displayed in most browsers when on any secure website. The browser not only shows you the trust chain, but it verifies the integrity of every certificate in the chain. It checks that none of the certificates in the chain has expired or has been revoked, meaning the private key was stolen or made public which makes the certificate basically invalid.

Digital certificates also have a regular, readable name, technically called a "Subject". For web sites, the subject name of the certificate securing the web site also must match the domain name of the web site. Finally - and crucially - **browsers and web client stacks will decline connections to web sites secured by a self-signed certificate**. The assumption is that without a separate issuer, no digital certificate can be fully trusted.

Timeout Settings

Kinetic uses default timeout settings to prevent frozen transactions from locking your system. If you typically process a large volume of data, you must increase these timeout settings to prevent the Kinetic application from prematurely stopping transactions before they complete.

Adjusting Timeout Settings

You adjust these settings in the **host.config** file. This configuration settings file defines the settings used by the application server that runs the Kinetic system. You typically adjust the timeout settings in this file, as they only affect transactions run by Kinetic . Available settings:

- **TransactionMaximumTimeout** - Defines the maximum time all transactions can run. If you enter a transaction time longer than this value, the system reduces the transaction time to this maximum value. Enter this value in **Hours : Minutes : Seconds**.
- **TransactionDefaultTimeout** - Defines the default time each transaction can run. If you do not specify a transaction time, the system uses this default value. Enter this value in **Hours : Minutes : Seconds**.

Be sure to thoroughly determine the consequences before you increase the duration limit on the host.config file. It may not be practical to raise this timeout limit. However when you receive the following errors, it might be appropriate to increase these timeout values:

- The transaction associated with the current connection has completed but has not been disposed. The transaction must be disposed before the connection can used to execute SQL statements.
- Cannot access a disposed object transaction.
- Transaction scope nested incorrectly.

Some part transactions and serial number processing may require a five hour timeout durations. Because this exceeds the standard ten minute duration, you can adjust the host.config file to handle these five hour transactions. This features helps you determine the cause of timeout issues for these users.

Even though you can set the TransactionMaximumTimeout setting to a longer timeout duration, the framework first uses the lower timeout durations defined in TransactionDefaultTimeout or transaction scope values. If you wish to test a system using the five hour duration, you need to adjust the host.config or transaction scope values to handle the longer time limit as well.

You can also adjust timeout values in the reportserver.config file, the .sysconfig file, the Task Agent Configuration application, and on the SSRS Site. These settings define timeout durations for transactions that the host.config file does not monitor.

SSRS Site Timeout

If you regularly run large reports, set up SQL Server Reporting Services (SSRS) to either use a longer report timeout duration or indicate SSRS should never timeout reports. To do this, modify options within the Site Settings page on your report server.

1. On your server, run the **Reporting Services Configuration Manager**.
2. In the Reporting Services Configuration Connection window, enter the **Server Name** and a **Report Server Instance** for the server that handles SSRS reporting for your system. Click **Connect**.
3. In the left pane, click the **Report Manager URL** icon. The Report Manager URL screen displays.
4. Click the **URLs** hyperlink to display SQL Server Reporting Services in your internet browser.
5. A login window displays. Enter a Windows user account that has permissions to view the SSRS site. Click **OK**.
6. On the Home page for SQL Server Reporting Services, in the upper right corner, click the **Site Settings** hyperlink.
7. On the Site Settings page, locate the **Report Timeout** radio button options. Select one of the following options:
    - Select the **Do not timeout report** option to prevent SSRS from stopping reports from generating.
    - Select the **Limit report processing to the following number of seconds** option to increase how long SSRS can run while it generates reports. Then enter how many more seconds each report can run before it timeouts.
8. Click **Apply**.

Minimum Number of Threads

Several processes, like MRP and Scheduling, use threads to improve performance. You split one process run into multiple threads so it takes less time to complete. Users can change the number the threads each process requires, controlling the server resources each process uses. However if not enough threads are available, these changes can slow performance.

To make sure all processes have enough threads, define the minimum number of threads that must run for the entire system. If the system requires more than this minimum value to handle the load, it can create additional threads. When a process runs, the system will then be ready to create those threads if needed to improve performance.

Do this by adding a row to the **ICE.SysConfig** table that defines how many threads will be available for all processes. Because ICE.SysConfig is a system table, you can add this row in both on-premise and cloud environments. Do the following:

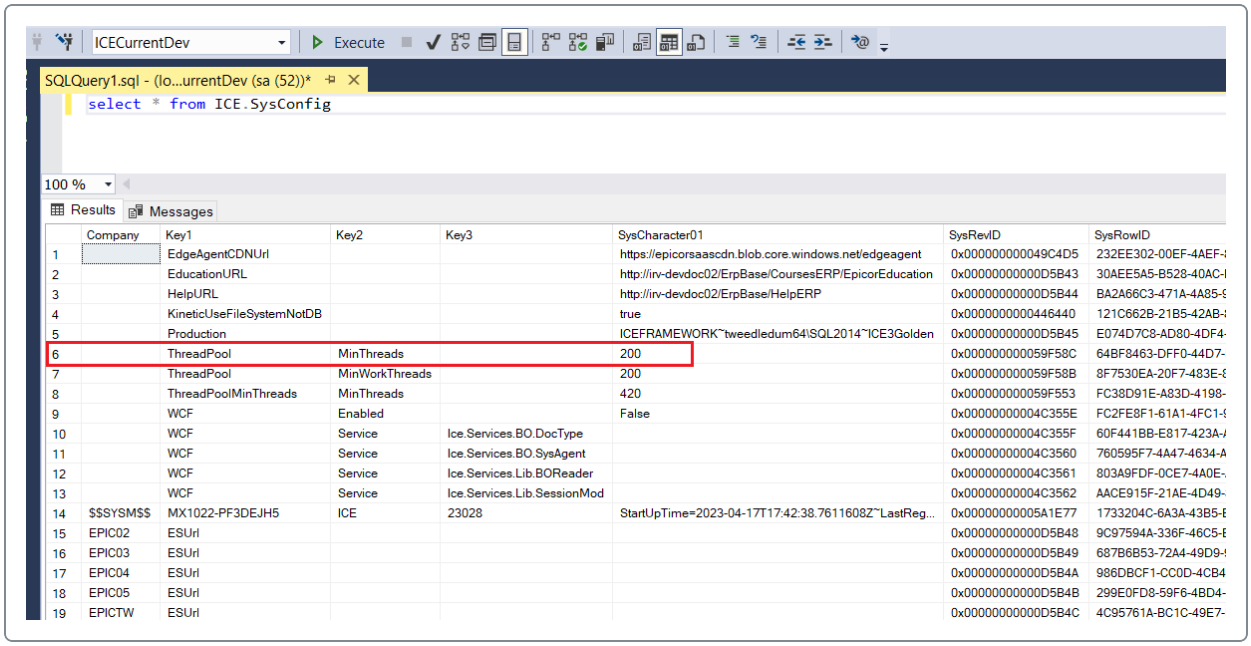
1. Launch **SQL Server Management Studio**.
2. Create a new query. Enter this script:

```
ICE.SysConfig (Key1, Key2, SysCharacter01) VALUES ('ThreadPool',
'MinThreads', 200)
```

The above code is an example script that causes the system to quickly create as many as 200 threads that improve performance. These are the first 200 threads the system immediately creates, but system can create more threads if needed to handle the load. Substitute the "200" value with the minimum number of threads you require on your system.

3. Select the **Execute** button.

4. The script adds the row to the ICE.SysConfig table and sets the minimum threads for the system:



	Company	Key1	Key2	Key3	SysCharacter01	SysRevID	SysRowID
1		EdgeAgentCDNUrl			https://epicorsaascdn.blob.core.windows.net/edgeagent	0x0000000000049C4D5	232EE302-00EF-4AEF-
2		EducationURL			http://irv-devdoc02/ErpBase/CoursesERP/EpicorEducation	0x00000000000D5B43	30AEE5A5-B528-40AC-
3		HelpURL			http://irv-devdoc02/ErpBase/HelpERP	0x00000000000D5B44	BA2A66C3-471A-4A85-
4		KineticUseFileSystemNotDB			true	0x0000000000446440	121C662B-21B5-42AB-
5		Production			ICEFRAMEWORK~tweedledum64\SQL2014~ICE3Golden	0x00000000000D5B45	E074D7C8-AD80-4DF4-
6		ThreadPool	MinThreads		200	0x000000000059F58C	64BF8463-DFF0-44D7-
7		ThreadPool	MinWorkThreads		200	0x000000000059F58B	8F7530EA-20F7-483E-
8		ThreadPoolMinThreads	MinThreads		420	0x000000000059F553	FC38D91E-A83D-4198-
9		WCF	Enabled		False	0x00000000004C355E	FC2FE8F1-61A1-4FC1-
10		WCF	Service	Ice.Services.BO.DocType		0x00000000004C355F	60F441BB-E817-423A-
11		WCF	Service	Ice.Services.BO.SysAgent		0x00000000004C3560	760595F7-4A47-4634-A
12		WCF	Service	Ice.Services.Lib.BOReader		0x00000000004C3561	803A9FDF-0CE7-4A0E-
13		WCF	Service	Ice.Services.Lib.SessionMod		0x00000000004C3562	AACE915F-21AE-4D49-
14	$$SYSM$$	MX1022-PF3DEJH5	ICE	23028	StartUpTime=2023-04-17T17:42:38.7611608Z~LastReg...	0x00000000005A1E777	1733204C-6A3A-43B5-
15	EPIC02	ESUrl				0x00000000000D5B48	9C97594A-336F-46C5-
16	EPIC03	ESUrl				0x00000000000D5B49	687B6B53-72A4-49D9-
17	EPIC04	ESUrl				0x00000000000D5B4A	986DBCF1-CC0D-4CB4
18	EPIC05	ESUrl				0x00000000000D5B4B	299E0FD8-59F6-4BD4-
19	EPICTW	ESUrl				0x00000000000D5B4C	4C95761A-BC1C-49E7-

This minimum setting is applied to the system Host in runtime. If you wish to change this value later, update the row created in the ICE.SysConfig table and set it to the new minimum number of threads you need. Then activate this change by stopping and restarting the system application pool.

Trace Flags

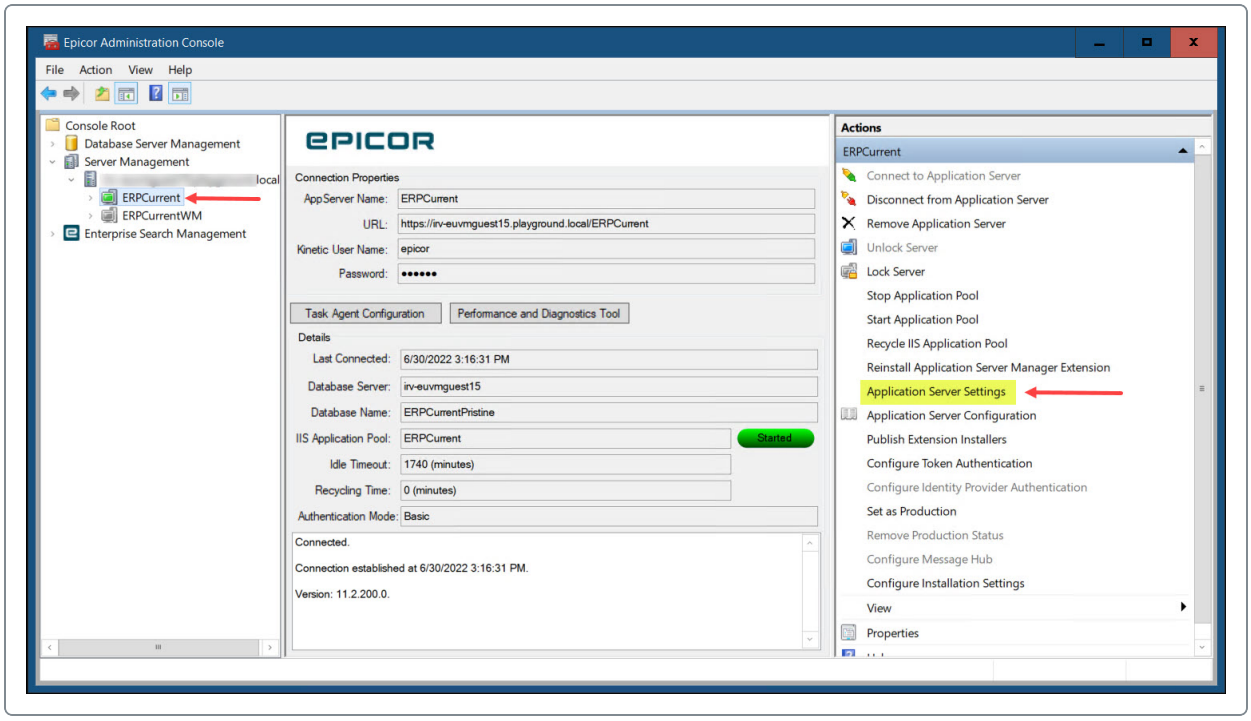
Activating Trace Flags

You activate trace flags in two ways. You can update the server log or you can activate trace flags within the Epicor Administration Console.

Epicor Administration Console

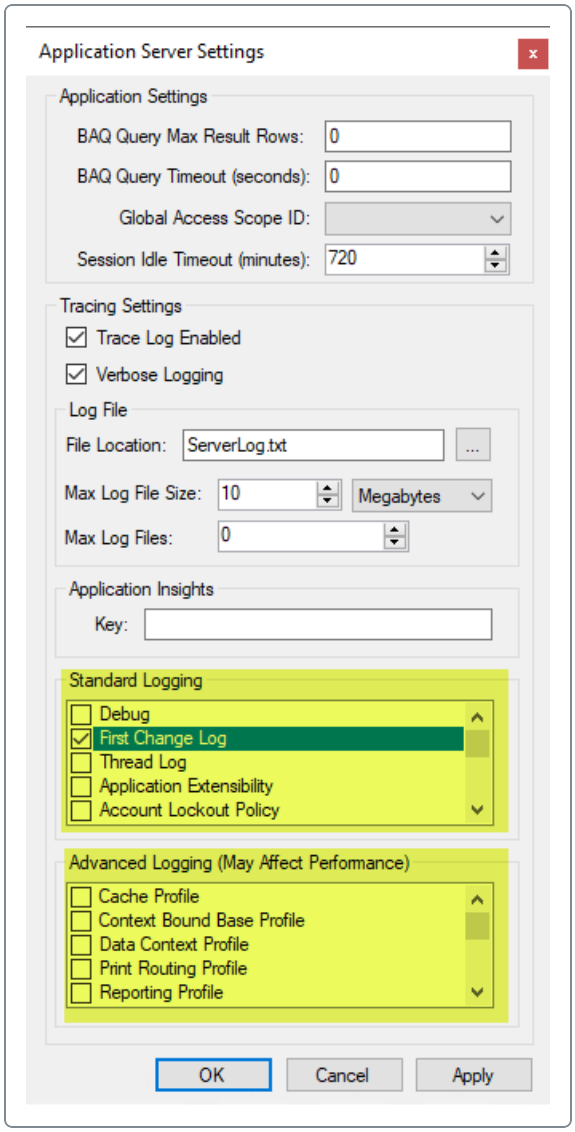
To activate trace flags within the Epicor Administration Console:

1. Go to the server.
2. Launch the **Epicor Administration Console**
3. Go to the **Tree View**.



4. Expand the **Server Management > [YourServerName] > [YourApplicationServer]** node.
5. Select your application server.
6. Go to the **Actions** pane and select **Application Server Settings**.

7. The Application Server Settings dialog displays. Select the **Standard Logging** and **Advanced Logging** trace flags you want to activate.



8. Select **OK**.

The server log generates using the trace flags you selected to monitor.

> Review the complete last of trace flags later in this article. Some Advanced Logging trace flags can affect performance. You may want to run these trace flags for a limited time period and then shut them off.

The Server Log

To activate trace flags directly on the server log:

1. Go to the server.
2. Using the **File Explorer**, go to **C:\<YourKineticInstallation>\<YourKineticVersion>\Server**
3. Using a text editor, open the **AppServer.config** file.
4. First enable logging. Change the Trace disabled value to false:

```
<configuration>
 <Trace disabled="false">
```

5. Now enter the trace flags that you will run. Use this syntax:

```
<add uri="trace://ice/fw/sysagenttask" />
```

6. Substitute the bold value above with the uri for the trace or profile you wish to activate. You can review the trace flags and their Uri values in the next section.
7. **Save** the AppServer.config file.

Review the complete last of trace flags below. Some Advanced Logging trace flags can affect performance. You may want to run these trace flags for limited time period and then shut them off.

Trace Flags List

This section describes the trace flags you can activate in the server log.

Trace Name	Uri	Purpose
Account Lockout Policy	trace://ice/fw/accountlockoutpolicy	Tracks failed login attempts that locked a user account.

Trace Name	Uri	Purpose
Application Extensibility	trace://ice/fw/applicationextensibility	Tracks activity for services you have extended with additional logic and/or database columns. It measures when the system calls an extension method and how long it took to run.
Assembly Loading Profile	profile://system/assemblyloading	Displays the items and options that load when the Kinetic system launches.
Auto Printing Log	trace://ice/fw/autoprint	Tracks the activity for any Business Process Management (BPM) methods that run automatic printing. They have the Auto Print widget in their method flows.
BAQ Logging	trace://ice/fw/DynamicQuery	Tracks the activity for business activity queries (BAQs) when they run against the Kinetic database.
BAQ Statement Profile	profile://ice/fw/DynamicQuery/BaqStatement	Displays the SQL statements that generate when business activity queries (BAQs) run against the database.

Trace Name	Uri	Purpose
BO Reader Log	trace://ice/fw/boreader	Tracks any messages from calls that generate from the BO Reader service. These calls return data from various parts of the system.
BPM Logging	trace://ice/fw/BPM	Tracks the activity for Business Process Management (BPM) method, data, and updatable BAQ directives.
Call Context Log	trace://system/callcontext	Tracks non-standard information sent between clients and the server. It displays the data sent to a server method that then returns to the client in the CallContextHeader.
CDC Log	trace://ice/fw/cdc	Tracks Epicor Change Data Capture (CDC) activity, displaying information about advanced custom integrations. Several features require these integrations. Collaborate also requires these integrations to generate notifications.

Trace Name	Uri	Purpose
Change Log	trace://ice/fw/changelog	Tracks calls that get or retrieve ChangeLog data. It displays data similar to the Change Log audit feature within Kinetic.
Context Bound Base Profile	profile://ice/fw/contextboundbase	Tracks two areas of activity. It tracks the TaskBase, which is the base class for task agent tasks. It records errors that occur when the system tries to update the progress status of a task. It also tracks the ContextBoundBase, which is the base class for services and other classes. It tracks information about each class and the datacontext each class uses.
Database Hits Profile	profile://system/db/hits	Displays database information such as database query count, database cache hits, and database time. The trace flag records each server call.

Trace Name	Uri	Purpose
Data Context Profile	profile://ice/fw/datacontext	Displays information about each datacontext such as the context ID and the connection SPID. Then for each database connection, it also displays EpiConnection class information such as the local identifier, SPID, and stack trace details.
Data Context	trace://ice/fw/datacontext	Displays information about when the system creates or disposes each EpiDataContext transaction. It also displays the context ID and the connection SPID for each EpDataContext. Then for each database connection, it also displays EpiConnection class information such as the local identifier and SPID.
Database Expression Compiler Profile	profile://system/data/dbexpressioncompilerquerycache	Displays details about compiled database queries that this system caches. The trace flag records the cache category, such as InvokeSingleQueryCache. It also displays the cache count.

Trace Name	Uri	Purpose
Debug	trace://diagnostics/debug	Tracks performance information such as performance counters and extensions.
Dispose Log	trace://ice/fw/disposable	Tracks OperationBound classes that the system CANNOT dispose.
EDI Print	trace://ice/fw/ediprint	Tracks both information and errors that occur when users generate Electronic Data Interchange (EDI) reports.
EF Compiled Query Profile	profile://system/data/efcompiledquerycache	Displays when the system caches a compiled query, including the cache count and other details.
EPI Provider Log	trace://system/db/epiprovider	Tracks when an EpiConnection options, closes, and disposes. If an operation DOES NOT run the EpiConnection, this flag records this information.
EPI Provider Profile	profile://system/db/epiprovider	Tracks when an EpiConnection options, closes, and disposes. If an operation DOES run the EpiConnection, this flag records this information.
Extensibility Log	trace://ice/fw/extensibility	Tracks activity for any system extensions added to your environment.

Trace Name	Uri	Purpose
First Chance Log	trace://diagnostics/firstchance	Tracks the first chance exception errors from your SQL server. It tracks deadlock errors and any other SQL exception. This log option can return a lot of information.
Host Log	trace://system/host	Tracks who, when, and what user account and client machine logged into the server. It also tracks all the changes made to DB Tables, the DataModel, and the AssemblyStore.
Import Service Profile	profile://ice/services/import	Displays the definition for each service in your environment. You can then import this service profile into another environment to register it.
Kinetic DB Hits	trace://system/db/hits	Tracks client activity with the system database. You can then see both who accessed the database and when they did it.

Trace Name	Uri	Purpose
Kinetic Log	trace://ice/fw/kinetic	Tracks the application activity within your environment. This tracing option shows which applications ran and who launched them.
License Log	trace://ice/fw/license	Tracks which Kinetic module licenses are active.
Message Hub Log	trace://ice/fw/messagehub	Tracks the messages that generate for SaaS network printing. This log option is only available in Cloud environments.
Notification EFC Log	trace://ice/fw/notification/ECF	Tracks the Enterprise Fabric Connectivity activity that occurs against this fully qualified network domain address.
Notification Log	trace://ice/fw/notification	Tracks the report and process alert notifications that users generate in your Kinetic environment.
Notification Profile	profile://ice/fw/notification	Displays the notification definition defined within your Kinetic environment.

Trace Name	Uri	Purpose
Operation Initialize Time	trace://ice/fw/initialize	Tracks how long it takes to launch Kinetic services (also called business objects). You can then determine the performance of these services.
Performance	trace://ice/fw/perf	Tracks how efficiently the system runs through a series of performance indicators. The trace flag includes how long it takes to both initialize and run operations. Use this log setting to locate processes, BPM methods, custom layers, BAQs, and other items that may be reducing performance.
Print Routing Profile	profile://ice/fw/printrouting	Displays reports that automatically generate and print. Users create routing rules to run reports on a regular basis. Typically when a routing rule condition is met, the report prints using an output action.
Reporting Log	trace://ice/fw/reporting	Tracks the reports users generate and print. You see the report name, the user that launched the report, and the date/time it was run.

Trace Name	Uri	Purpose
Reporting Profile	profile://ice/fw/reporting	Displays the report definition for your environment. You can see the SSRS report server and other report system information.
Rest API Log	trace://ice/fw/restapi	Tracks the Application Programming Interfaces, or API, calls users make against REST services. You see each API call and the service it activated.
Security Profile	profile://system/security	Displays several aspects of the security settings defined within your environment, such as authentication and identification. Use this log to check on authenticated users, password changes, and other security activities.
Service Caller Log	trace://ice/fw/servicecaller	This trace flag retrieves the service types for both operations and business objects.
Session Log	trace://ice/fw/session	Tracks the user sessions running in the application server. You can see who launched the session, when it started, and when the session stopped.

Trace Name	Uri	Purpose
Session Settings Profile	profile://ice/fw/sessionsettings	Displays the settings your environment uses to run sessions within your application server.
SignalR Log	trace://ice/fw/signalr	This trace flag option is only available in Cloud environments. It works together with the SignalR Profile to determine the logging level you need. The log tracks server to client communication. Use it to troubleshoot issues that may occur when a cloud environment interacts with Azure. This trace log tracks Warnings, Errors, and Critical Failures.
SignalR Profile	profile://ice/fw/signalr	This trace flag option is only available in Cloud environments. It works together with the SignalR Log to determine the logging level you need. Like the log, this profile tracks server/client communication. It displays debug and informational messages. If you want to see all cloud server to client communication, you MUST activate both the SignalR Log and the SignalR Profile.

Trace Name	Uri	Purpose
SQL Query Detail	profile://system/db/epiprovider/sqltext	Tracks commands that query SQL server data. These commands pass through the Entity Framework. The trace log displays the SQL statements that generate from these commands.
System Agent Task Log	trace://ice/fw/sysagenttask	Traces the flow of task-related activity on the server.
System DB Hits	profile://system/db/stacktrace	Displays every call the application server sends to the SQL server database. This log captures a high volume of data, so DO NOT leave this trace flag running on your system for very long. It will affect system performance.

Trace Name	Uri	Purpose
System Table Methods	profile://ice/fw/tableset	Tablesets both hold updated data and expose this data. Mainly used for troubleshooting, this trace flag records a lot of information. It records performance counters also tracks interactions with runtime tablesets as users add, remove, and update dataset rows during a server call lifecycle. This log captures a high volume of data, so DO NOT leave this trace flag running on your system for very long. It will affect system performance.
Thread Log	trace://diagnostics/thread	A thread is an instruction set that runs an application. Each thread sends a process action to the server. While generating these process actions, the application server can both run and close down operating system thread to improve performance. This flag monitors unexpected errors and displays how long each thread took to process. It DOES NOT show what work each thread does within the system.

Trace Name	Uri	Purpose
Trigger Hits	trace://ice/fw/trigger	Tracks the triggers which launch events that update data, launch a process, run a calculation, and other event actions.
Update Ext Profile	profile://ice/fw/updateext	The UpdateEXT method sends calls that specify the minimum information the system needs to update a row. It uses the data it can access on the server to recreate the full, required tableset and then calls the standard Update method. This trace flag tracks the actions each UpdateEXT method requires to call the standard Update method.
Version Check	trace://ice/fw/versioncheck	Tracks the Kinetic versions of the application server and the database. When these versions do not match, errors display on both the client and the server logs.

Managing Telemetry

To help troubleshoot issues, analyze trends, and improve usage, Epicor will, unless you affirmatively opt-out, automatically collect and process non-personal telemetric data from Kinetic. The data includes active users, authentication modes, active sites, and open views. The collected information is non-personal, non-identifiable, and subject to the Epicor Privacy Policy which is hereby incorporated by reference.

Russia and China do not participate in the telemetry data collection process due to regulatory requirements in these countries.

Kinetic does this by gathering **ConnectionString** data. This ConnectionString data is sent to Application Insights for review by Epicor. When you deploy an application server in the Administration Console, the Telemetry and License Data message displays, informing you that the telemetry tracking is enabled.

If you choose to decline participation in this data collection process, you may opt-out at any time. Open Administration Console and select the **Opt Out** check box in **Company Properties** to disable this service.