HEXAGON

ICS Integrity

Installation Guide

2023 (7.3)
February 2023

Contents

About the Product Documentation

Integrity Software Suite provides many resources to help you use the product, including a *documentation web site https://docs.hexagonali.com/*:

Readiness Checklist

Provides guidance to ensure your environment is prepared for the installation and deployment of the product. It is included with the *Installation Guide*.

Installation Guide

Provides detailed planning and installation guidance, as well as some initial required configuration and troubleshooting procedures.

Implementation Guides

Provides detailed information about a source of data for the product. With the breadth of the product, there are many Implementation Guides to help you get the details you need about the specific data sources in your environment.

Administration Guide

Provides strategy and best practice information for configuring and managing the product. This book defines terminology and provides the concepts and procedures you need.

User Guide

Provides product concepts and usage information, including step-by-step guidance for common tasks.

Help

Provides a comprehensive, integrated online resource that includes all the information from the *User Guide* and *Administration Guide*. For more information about using the documentation web site, see the *Documentation Site Help https://docs.hexagonali.com/access/sources/AITM/topic?ait:code=946343*.

Conventions

The documentation uses consistent conventions to help you identify items. The following table summarizes these conventions.

Convention	Use
Bold	▪ Window and menu items ▪ Technical terms, when introduced
Italics	▪ Book titles ▪ Variable names ▪ Emphasized words
Fixed Font	▪ File and folder names ▪ Commands and code examples ▪ Text you must type ▪ Text (output) displayed in the command-line interface
Color	▪ Links
>	▪ Submenu selections, such as Generate Reports > All
Brackets, such as [value]	▪ Optional parameters of a command
Braces, such as {value}	▪ Required parameters of a command
Logical OR, such as value1 | value2	▪ Exclusive parameters. Choose one parameter.

Technical Support

Please contact us with your questions and comments. We look forward to hearing from you. If you need assistance with an issue, contact Technical Support.

Support Portal

Log into the Support Portal at any time to enter new cases and track existing cases: *smartcommunity.hexagonppm.com https://smartcommunity.hexagonppm.com/*

Website

www.pas.com http://www.pas.com

SECTION 1

Introduction

Today’s automation systems have become incredibly complex, with thousands of measurements, multiple integrated applications, and more interoperability than ever before. This combination of greater complexity and continual change leaves facilities vulnerable to the effects of undocumented and unapproved changes to system configuration.

In addition, securing each industrial control system (ICS) requires knowing and tracking a complete inventory of all proprietary ICS and traditional information technology (IT) assets. Only with a comprehensive inventory that includes configuration data can companies secure against unauthorized change, achieve a sufficient compliance standard, mitigate risk, and ultimately improve process safety.

Unfortunately, traditional IT-based tools provide little support as they do not collect the up-to-date inventory and deep proprietary configuration data required for established security best practices. Without a comprehensive, evergreen inventory, it is difficult to detect unauthorized changes due to malicious attack or inadvertent engineering updates, obtain visibility into proprietary control system vulnerabilities, or maintain compliance against regulatory or corporate standards.

The Integrity Software Suite (Integrity) provides the integrated solution you need to address your automated asset management requirements and your ICS security demands.

SECTION

What Is Automation Integrity?

Automation Integrity is an enterprise application for automation asset management at industrial plants. It aggregates and contextualizes configuration databases, programs, and user interfaces. It also simplifies the visualization and the management of information in automation systems.

Automation Integrity comprehensively minimizes human error by identifying configuration defects, preventing unexpected plant incidents and shutdowns. In today's competitive production environment, proper documentation and change tracking are essential for effective troubleshooting, faster problem resolution, and incident avoidance. Focusing on minimizing human error, Automation Integrity improves plant safety and reduces operating risk.

Map Automation Systems

Automation Integrity helps you visualize complex configurations and interdependencies between disparate systems. Diagrammed mapping traces signal genealogy from field instrumentation to advanced process control. With this visual mapping, you can identify related systems and controls to make informed decisions and more effectively evaluate potential changes and their effects.

Maintain standard settings

Sensor Data Integrity compares thousands of configuration settings from AMS device tags to templates you define that contain your best practice standard settings. creates defects for mismatched settings and missing templates to help you maintain and verify your configuration for sensor instruments.

Document Configuration and Track Changes

Automation Integrity uses automated uploads of the latest configuration information from disparate systems to build a comprehensive database of configuration data. With this data, Automation Integrity quickly identifies configuration changes and helps you investigate and determine whether these changes were approved or unapproved.

Retain System Knowledge

With Automation Integrity, plant personnel can securely access configuration information, automation procedures, control logic, DCS parameters, and other relevant information. This knowledge resource helps your team identify potential issues, understand how and why systems are configured, and bring together important details to make informed decisions.

Automate Work Processes

Automation Integrity provides a powerful workflow system to help you manage change in your environment. You can create and implement automated workflow processes with checklists and approval requirements as needed. These workflows can provide management of change (MOC) cases to track proposed changes, implemented changes, and to support automatic reconciliation of changes.

Inventory System Utilization and Available Spare Capacity

With Automation Integrity, you can identify, reserve, and manage spare capacity of points within your control systems.

SECTION

How These Products Help You

The Integrity Software Suite is the leading solution for ICS security, process safety, and asset reliability in the energy, power, and process industries. From configuration management and compliance to change tracking and vulnerability management, the Integrity platform provides complete visibility into your industrial control systems enabling greater operational efficiency, improved foundational ICS security, and reduced operational risk. The following sections highlight several important benefits.

Improves Productivity and Minimizes Human Error

Automation Integrity improves productivity of automation personnel by 20 to 50 percent, which also improves profitability. With Integrity, you can decrease the time required to investigate and recover from process upsets. In addition, Automation Integrity minimizes human error by identifying and eliminating configuration defects to prevent unexpected plant incidents and shutdowns. With this solution, you can identify and revert unapproved configuration changes before they cause problems and increase safety risks.

Reduces Inventory and Documentation Effort by 70% or More

Automation Integrity provides inventory management across both IT-based systems and proprietary control systems. This task is often performed manually, and it is difficult to keep up to date. With its automated data collection and global views, Integrity greatly reduces the time and money dedicated to identifying and documenting the assets you have.

Manages Across All Major Control System Manufacturers

PAS has an extensive list of more than 75 different control system asset models that the Integrity platform uses to gather essential configuration information for viewing and analyzing in a common format. Automation Integrity provides scalability from base to higher-level functionality. It also facilitates capturing and contextualizing data from disparate systems into a common format for use within the Integrity Software Suite. ICS Integrity is highly scalable, enterprise-class software built on the Integrity platform, which is deployed at hundreds of sites across the world.

Hardens Industrial Control Endpoints Against Cyber Threats

ICS Integrity provides powerful vulnerability management and configuration management features to help strengthen industrial control endpoints against threats and attacks. With this solution, you can compare your assets to known vulnerabilities and then use the custom workflow to evaluate patches and apply them as needed, or to make other changes to mitigate the risk. ICS Integrity also detects inadvertent engineering changes or malicious attacks across your inventory so you can start a workflow case to investigate the changes and revert as needed.

Reduces Compliance and Operational Efforts by up to 90%

Maintaining internal and regulatory compliance can put demands on your time that impacts other operational activities and projects. ICS Integrity maintains the evidentiary proof of compliance adherence by capturing information that feeds these compliance requirements. Integrity automates audit-ready compliance through reporting and process automation, which can also facilitate Process Safety Management (PSM) requirements. With ICS Integrity, you can also eliminate environmental excursions caused by inadequate configuration management and management of change.

Prevents Unplanned Downtime

ICS Integrity automatically creates searchable electronic documentation and reconciles configuration changes during projects. This automation improves quality through collaboration and reduces migration and systems integration projects time by up to 10 percent. With these tools and systems in place, you can prevent unplanned downtime and potential system conflicts due to unidentified dependencies.

SECTION

What Is ICS Integrity?

ICS Integrity, part of the Integrity Software Suite, leverages the capabilities of the Integrity platform to embrace ICS cybersecurity standards-based requirements for process control network (PCN) inventory, configuration change, vulnerability and compliance management, as well as backup and recovery. ICS Integrity provides a holistic view of ICS cybersecurity across your enterprise.

ICS Integrity hardens security for the most mission-critical assets in a plant, the industrial control systems. The product works across the multi-vendor automation environment, providing enterprise scalability, performance, and platform independence.

Inventory Management

ICS Integrity maintains a complete industrial endpoint inventory that includes both production and IT-centric assets. This complete inventory of IT and proprietary system configuration data includes control strategies, I/O cards, firmware, installed software, and any custom data.

Configuration Management

ICS Integrity monitors, detects, and remediates unauthorized configuration changes with the following capabilities:

- Changes: Monitors for unauthorized changes to control strategies, inventories, asset configuration, and logical and graphical files. Automates remediation actions through workflows based on asset value and risk guiding operations, compliance, and cybersecurity responses.
- Policies: Maintains security and operational imperatives through configuration policies, alerts, and workflows using asset-specific incident responses.
- Baselines: Defines the set of configuration data required for ICS cybersecurity, compliance, governance, and operations change monitoring.

Vulnerability Management

ICS Integrity provides continuous vulnerability management with automated assessments of industrial control system assets, remediation workflows, and closed-loop patch management. The patch management features assess the applicability and impact of Microsoft patches and vendor bulletins. ICS Integrity provides custom workflows to ensure consistent remediation and mitigation activity and reporting. To inform your cyber risk management decisions, ICS Integrity also provides dashboards and trend views.

Compliance Management

ICS Integrity enables compliance with NERC-CIP, ISA/IEC 62443, NEI 08-09, NIST, and other regulations. You can audit and report on internal and regulatory compliance requirements. ICS Integrity provides relevant and actionable information to the right people at the right time - including inventory, alerts, user authentication events, configuration details, change history, and workflow documentation.

Backup and Recovery

In the event of a worst-case scenario, ICS Integrity speeds recovery with backups of critical control system data and quickly enables restoration of control system operations. ICS Integrity captures full configuration backups on a regular basis, which helps reduce recovery times.

SECTION 2

Installing Integrity

This section outlines the installation and related configuration tasks for initially setting up Integrity. Additional configuration information is also available in the Administration Guide for other system customization tasks and capabilities.

If you are upgrading an existing Integrity installation, you do not need to perform many of the tasks in this section. For more information about upgrading an existing Integrity installation, see *Upgrading from a Previous Version* (page 47).

Initial Installation Steps

Before you install Integrity, use the Readiness Checklist to make sure your systems are equipped with the hardware and software required for running Integrity. You should also understand how you will deploy Integrity in your environment.

Integrity is very flexible and can be deployed in many ways, depending on your network architecture, firewalls, and security policies. For more information about requirements and deployment options, see *Completing the Readiness Checklist* (page 59).

NOTE Actual system requirements are based on the number and types of assets included in the deployment.

The following steps allow you to plan for, install, and configure Integrity for the first time. These steps guide you through the remaining sections of this document.

1. Verify all computers meet (or exceed) the requirements as stated in the Readiness Checklist for the version of software being installed. For more information, see *Readiness Checklist* (page 59).
2. On each computer where you will install the Integrity Server or Integrity Data Collector, you can update the hosts file to include the IP address and host name for the SQL Server computer it will communicate with, if needed. For more information, see *Adding the SQL Server Host Name and IP Address to the Hosts Files* (page 15).
3. On each computer where you will install one or more Integrity components, open the ports used by those components. For more information, see *Open Ports Required by Integrity* (page 16).
4. Use the Ping command and Telnet to test communication between the computers where you will install Integrity components. For more information, see *Testing Communication between Integrity Computers* (page 16).
5. If you want to ensure permissions are set as needed, create the folder where you will install Integrity on each computer and set the permissions on that folder. For more information, see *Creating the Integrity Installation Folder* (page 17).
6. If you are upgrading an existing Integrity database, check that the existing database compatibility is set above SQL Server 2000 to the highest compatibility possible. For more information, see *Checking the Compatibility Level in SQL Server* (page 44).

7. Verify that the Integrity Web servers have no underscores in the host name. If they do, rename the host. For more information, see *http://support.microsoft.com/kb/909264 http://support.microsoft.com/kb/909264*.
8. Ensure that both the Application and Web Server Roles and the associated services/features are added on the Integrity Servers. For more information, see *Configuring Windows Web Server Roles and Features for Integrity* (page 17).
9. On the SQL Server computer, use SQL Server Management Studio for the following tasks:
   a. Make sure the person running the Integrity installation program has at least the dbcreator server role where the Integrity database will be created. If using multiple databases, this person must have at least the setup_admin server role. For more information, see *Configuring Roles and Permissions in SQL Server* (page 41).
   b. Disable CLR strict security. For more information, see *Updating SQL Server CLR Strict Security and Cost Threshold Settings* (page 20).
   c. Allocate the appropriate amount of memory to SQL Server: 75% of memory for systems with 24GB of RAM and above, or 50% if system RAM is below 24GB. For more information, see *Performance Issues - Checking SQL Server Memory* (page 45).
10. PAS by Hexagon recommends that you turn off the Windows User Account Control (UAC) feature.
11. Turn off the Windows Firewall (or alternatively, enable Notifications if the firewall blocks a program for all types of network, such as Public, Domain, or Work).
12. If you need to save control maps, check that Visio is installed. Open a Visio file (*.vsd) and verify the software product is present, licensed, and activated. For more information, see *Issues with Report Generation for PDF or Visio* (page 45).
13. Create a PAS folder in a root directory (for example, C:\ or D:\). Give permissions to the PAS folder and propagate to children (Network Service, IIS_IUSRS, Authenticated Users and any Application Accounts).
14. Enable FILESTREAM (requires SQL Server 2008 or later). For more information, see *FILESTREAM Configuration Recommendations* (page 21) and *Enabling FILESTREAM* (page 22).
15. Install the Full-Text and Semantic Extractions for Search feature in SQL Server. This is an optional component of the SQL Server Database Engine. For more information, see *Installing Full-Text Search for SQL Server* (page 22).
16. Make sure that IIS X-frame options are set to allow. For more information, see *Setting IIS X-Frame-Options to Allow* (page 23).
17. Install Microsoft Excel 2010 or later on the web server if you want to run the hierarchical reports or if you use certain asset models.

    NOTE Some asset models, such as PAS Sensor Data Integrity or ABB Symphony Plus, require data imports from Excel files. See the individual asset model *Implementation Guide* to determine whether an individual model has this requirement to facilitate the transfer from Microsoft Excel, which may require Microsoft Access Database Engine (AccessDatabaseEngine.exe) on the data collector computers. The AccessDatabaseEngine.exe file is available in the following ways:

    - Additional Software link in the Integrity installation program
    - Installation folder after installing Integrity

- Available for download from *https://www.microsoft.com/en-us/download/details.aspx?id=13255* *https://www.microsoft.com/en-us/download/details.aspx?id=13255*

18. Install Integrity on each computer where you need a component. For more information, see *Installing Integrity for the First Time* (page 23).
19. Set the Admin Utility to run as administrator. For more information, see *Setting Integrity Admin Utility to Always Run as an Administrator* (page 40).
20. Start the Integrity Admin Utility. For more information, see *Using the Integrity Administration Utility* (page 24).
21. Validate your product license. For more information, see *Validating Your License* (page 24).
22. Create the Integrity database. For more information, see *Creating the Database* (page 26).
23. If you are using multiple databases, create the additional databases. For more information, see *Configuring Multiple Databases* (page 27). For more information about importing source assets using multiple databases, see *Importing Asset Models Using Multiple Databases* (page 31).
24. Configure the virtual directory for the Integrity Web application. For more information, see *Defining the Web Application (Integrity Web Interface)* (page 31).
25. On the SQL Server computer, use SQL Server Management Studio to make sure the Integrity service accounts have the required permissions. Then, assign the accounts to the Integrity services. Since the IntegrityAppPool for the Integrity web interface uses the Network Service account by default, make sure the NT Authority\Network Service account has the appropriate roles for the Integrity database. For more information, see *Defining Your Service Accounts* (page 32).
26. If you are installing ICS Integrity, import the PAS Cyber Integrity asset model and create an asset using this model to support the other ICS Integrity features you choose to use. For more information, see *Setting Up the Asset for ICS Integrity Features* (page 34).
27. Import an asset model for one type of asset. Integrity provides many asset models. To make sure Integrity is correctly installed and configured, initially import one asset model and add an asset of that type. For more information, see *Loading (Importing) an Asset Model* (page 35).
28. Add one or more assets for the imported asset model. For more information, see *Adding an Asset (Data Owner)* (page 36).
29. Run an import so you can view data for the added asset. You can select the Run Now option when scheduling an import to run the import immediately. For more information, see *Scheduling Data Imports* (page 36).
30. Create SQL Server Maintenance Jobs per Application. For more information, see *Setting Up SQL Server Maintenance Jobs* (page 41).

This initial installation and configuration ensures your database and user interfaces are connected and you can view data for the initial asset model. You should now import additional asset models, add your remaining assets, schedule imports, and review security for service accounts. You can also configure the asset explorer tree and perform other maintenance tasks. For more information about Integrity administration and additional configuration, see the *Integrity Administration Guide*.

SECTION

Preparing Your Environment for Integrity

Before installing Integrity software, you need to implement several changes to your system configuration to ensure success. Integrity relies on a distributed architecture, which uses the strength of internet protocols (IP) to allow remote devices to communicate and operate as if they were local. The fundamental approach in distributed architecture is the creation of discrete functions within a defined functionality scope. These functional elements exist in separate physical entities and communicate using IP.

Adding the SQL Server Host Name and IP Address to the Hosts Files

In a distributed environment, communication between computers on the Process Control Network (PCN) and computers on the Business Network (BN) can require IP addresses rather than relying on DNS. On each computer where you will install the Integrity Server or Data Collector, you can update the hosts file to include the host name and IP address for the SQL Server computer it will communicate with, if needed. This process enables communication between the Integrity Server or Data Collector and the database using the computer name without relying on DNS.

To edit the hosts file on a computer:

1. Run Notepad as an administrator.
2. Click **File > Open**.
3. Change the file types selection to **All Files (*.*)**.
4. Navigate to `%SystemRoot%\System32\drivers\etc\`, such as `C:\Windows\System32\drivers\etc`.
5. Select **hosts**, and then click **Open**.

   The information presented in the hosts file after the copyright and introductory comments provides mappings of IP addresses to host names. Each entry is on a separate line, with the IP address first, one or more spaces, and then the host name.

   The section of the comments right above where you should create your entries looks like the following example by default:

   ```
   #      102.54.94.97     rhino.acme.com          # source server
   #       38.25.63.10     x.acme.com              # x client host

   # localhost name resolution is handled within DNS itself.
   # 127.0.0.1       localhost
   # ::1             localhost
   ```

6. Add a line to the hosts file with the IP address and the name of the SQL Server computer. Type at least one leading space, the IP address, one or more spaces, and the host name. For example, using SQL Server on PASEXAMPLE at 192.168.23.30, add the following to the file:

   ```
    192.168.23.30       PASEXAMPLE
   ```

7. Click **File > Save**, and then close Notepad.

Open Ports Required by Integrity

In a distributed network deployment, Integrity requires certain ports to be open. For a complete list of the port requirements, see *Completing the Readiness Checklist* (page 59). The required ports include:

- ISS Server: TCP/IP port 25 for SMTP email notifications/reports
- SQL Server Default instance: TCP port 1433
- SQL Server Named instance: TCP port *xxxx* and UDP port 1434 where *xxxx* is the port number set for the named instance. This port number is determined by the network configuration
- Web Client: TCP port 80

Testing Communication between Integrity Computers

In configurations that use more than one computer, each computer needs to be able to communicate with the Integrity Server or SQL Server. After you add an entry in the hosts file on each computer where needed, you can use the Ping command to confirm access to that computer. Then, you can use Telnet to make sure the ports Integrity uses are open.

NOTES

- You may need to install or enable Telnet before you can use it. If Telnet is installed, you can enable it in Windows Start > Control Panel > Programs > Turn Windows features on or off.
- If you cannot use Telnet due to IT policy, use the following Powershell script:

  ```
  (new-object Net.Sockets.TcpClient).Connect("name", port)
  ```

  where `name` is the target computer name or IP address, such as 10.10.254.17, and `port` is the target computer port number, such as 1433.

To test communication from the local computer to a remote computer:

1. Click Windows **Start**, type `cmd` in the **Search** field, then press **Enter** to open the Command Prompt.
2. Type the following Ping command, where *PASEXAMPLE* is the name of the remote target computer, then press **Enter**:

   ```
   PING PASEXAMPLE
   ```

3. Verify that the Ping command does not time out, and that you receive a reply from the remote computer.
4. If you want to test communication by IP address, type the following Ping command, where *IPADDRESS* is the IP address of the remote computer, then press **Enter**:

   ```
   PING IPADDRESS
   ```

   If you want to have a computer ping itself, type PING 127.0.0.1 then press **Enter**.
5. Verify that the Ping command does not time out, and that a reply from the remote computer is received.
6. Use Telnet to test communication through the ports required by Integrity. The Telnet command uses the following format:

   ```
   telnet computername port
   ```

For more information, see *Open Ports Required by Integrity* (page 16).

Creating the Integrity Installation Folder

In some environments, permissions may not be set correctly on the folder where Integrity is installed. To help avoid potential permission issues, you can create the folder where you install Integrity and set the permissions on that folder.

To create the Integrity installation folder and set permissions:

1. Create the main folder for Integrity installation. The default location is `C:\Program Files (x86)\PAS\Integrity`.
2. Allow all permissions to that folder for the following groups and users:
   - Network Service
   - IIS_IUSRS
   - Integrity service account
   - Administrator user account used to install Integrity
3. To add or change permissions on the folder, complete the following steps:
   a. Open Windows File Explorer.
   b. Click the folder you created then press Alt + Enter to open the **Properties** window.
   c. Click the Security tab.
   d. If you need to add a user or group, click **Edit > Add**, specify the needed Object Types, Location, and Names, and then click **OK**.
   e. If you need to change permissions for a user or group, select the user or group, click **Edit**, select **Allow** for each permission needed, and click **OK**.
   f. Click OK to close the Properties window.
4. Make sure that all permissions are propagated to all folders. When all the permissions are set to **Allow** at the PAS folder, the permissions have propagated.

Configuring Windows Web Server Roles and Features for Integrity

The Integrity Application Server, also called the Web Server or Integrity Server, requires the following Windows roles:

- Application Server Role
- Web Server (IIS) Server Role

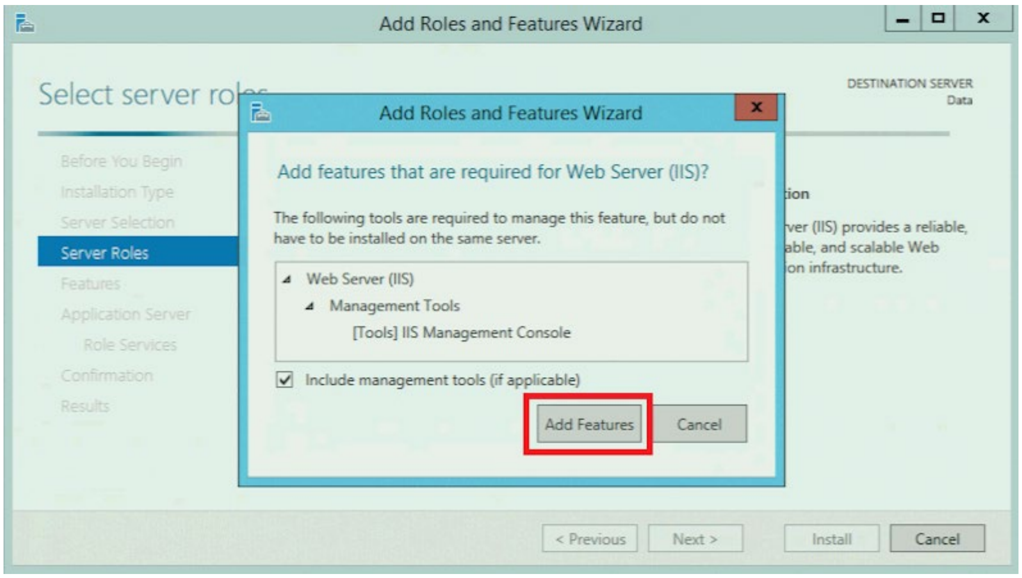
The Integrity Server also requires enabling several Internet Information Service (IIS) features. Perform the task outlined in this section on each computer where you install the Integrity Server.

NOTES

- To turn a Windows feature on, select the check box next to the feature. To turn a Windows feature off, clear the check box.
- When you enable some role services, Windows prompts you to enable other related features/services. Accept the additional related features/services.

To configure Windows roles and features on Windows Server 2012 or later:

1. Start Server Manager, and then click **Add roles and features**.
2. On the Before You Begin window, click **Next**.
3. On the Installation Type window, select **Role-based or feature-based** installation, and then click **Next**.
4. On the Server Selection window, select the target server (Integrity Server), and then click **Next**.
5. On the Server Roles window, select the **Application Server** and **Web Server (IIS)** check boxes.
6. If the Add Features for Web Server (IIS) window is displayed, select **Include management tools**, and then click **Add Features**.



7. On the Server Roles window, make sure that **WebDAV Publishing** under **Web Server (IIS) > Web Server > Common HTTP Features** is not selected or showing that it is installed, and then click **Next**.
8. On the Select Features window, click **Next**.
9. On the Application Server window, click **Next**.
10. On the Select Role Services window for Application Servers, select the **.NET Framework 4.8** check box, and then click **Next**.
11. On the Web Server Role (IIS) window, click **Next**.
12. On the Select Role Services window for Web Servers (IIS), select the following check boxes:
    - **Health and Diagnostics > Request Monitor**
    - **Performance > Dynamic Content Compression**
    - **Security > Request Filtering**
    - **Security > Basic Authentication**
    - **Security > Windows Authentication**

- **Management Tools > IIS Management Console**
- **Management Tools > IIS Management Scripts and Tools**
- **Management Tools > Management Service**

13. If the Add Features for Web Server (IIS) window is displayed, select **Include management tools**, and then click **Add Features**.
14. On the Confirm Installation window, click **Install**.
15. If any of your asset models require the **XPS Viewer** feature, ensure it is selected in the list of features. For more information, see your asset model *Implementation Guide*.
16. If you want to automate setting identical Server Roles and Features for multiple servers, use the **Export configuration settings** link on the Results window.
17. On the Results window, monitor the installation to make sure it is successful. After the installation is complete, click **Close**. Then, restart the server.

To configure Windows roles and features on Windows Server 2008:

1. Click Windows **Start > Control Panel > Programs**, and then click **Turn Windows features on or off.** The Server Manager window is displayed.
2. Click **Roles** in the left pane and make sure both the **Application Server** and **Web Server (IIS)** roles are added.
3. In the **Web Server (IIS)** section, click **Add Role Services**. The Add Role Services window is displayed.
4. Select the check boxes for the following services:

   NOTE Select the individual services. Do not select the check boxes for the service categories, which would select all services in that category.

   Common HTTP Features

   - Static Content
   - Default Document
   - Directory Browsing
   - HTTP Errors

   Application Development

   - ASP.NET
   - .NET Extensibility
   - ASP
   - CGI
   - ISAPI Extensions
   - ISAPI Filters

   Health and Diagnostics

   - HTTP Logging
   - Request Monitor

   Security

- Basic Authentication
- Windows Authentication
- Request Filtering

Performance

- Static Content Compression
- Dynamic Content Compression

Management Tools

- IIS Management Console
- IIS Management Scripts and Tools
- Management Service

5. Make sure that WebDAV Publishing under Common HTTP Features is not selected or showing that it is installed.
6. Click **Next**.
7. Click **Install**.
8. When done, on the Server Manager window, click **File > Exit**.

NOTE You may need to restart the server after adding the new services.

Updating SQL Server CLR Strict Security and Cost Threshold Settings

Starting with SQL Server 2017, the **CLR strict security** advanced setting is enabled by default. For more information, see *https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/CLR-strict-security http://docs.microsoft.com/en-us/sql/database-engine/configure-windows/clr-strict-security*.

To successfully install Integrity or migrate your Integrity databases on SQL Server 2017 or later, disable **CLR strict security**. After installing Integrity, you can enable **CLR strict security** if it is required for your environment.

To disable or enable CLR strict security:

1. Open Microsoft SQL Server Management Studio.
2. Connect to the SQL Server.
3. Run the following commands to disable CLR strict security:

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'CLR strict security', 0;
RECONFIGURE;
EXEC sp_configure 'show advanced options', 0;
RECONFIGURE;
```

4. After you install Integrity or migrate your Integrity databases, enable CLR strict security, if desired, by running the following commands:

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'CLR strict security', 1;
RECONFIGURE;
EXEC sp_configure 'show advanced options', 0;
RECONFIGURE;
```

Cost Threshold

The **Cost Threshold for Parallelism** option in SQL Server specifies the threshold at which SQL Server creates and runs parallel plans for queries. To prevent the query from using too many threads, you should update this value in SQL Server Management Studio.

To change the **Cost Threshold for Parallelism** value:

1. Open Microsoft SQL Server Management Studio.
2. Connect to the SQL Server.
3. Right-click on the SQL Server, and then click **Properties**. The Server Properties window is displayed.
4. In the left pane, click **Advanced**.
5. In the right pane under **Parallelism**, change the value for **Cost Threshold for Parallelism** to 50. The default value is 5.

SECTION

FILESTREAM Configuration Recommendations

FILESTREAM is a Microsoft product that enables SQL Server-based applications to store unstructured data, such as documents and images, in the file system. With FILESTREAM, applications can leverage the file system and at the same time maintain transactional consistency between the unstructured data and corresponding structured data.

Like most data-intensive applications, the Integrity database should be stored on a separated volume and not on the same volume with the operating system, SQL Server database, SQL Server log, tempdb, or paging file.

Microsoft also recommends the following best practices for FILESTREAM:

1. Always create the FILESTREAM data container that uses the FILESTREAM enabled database in a separate volume.
2. Use RAID 5 + stripping for the FILESTREAM data container as it provides excellent read, write, and fault tolerance. Follow this recommendation even though this is an expensive configuration.
3. It is a good practice to periodically perform disk defragmentation of the volumes which store FILESTREAM data.
4. Disable indexing on FILESTREAM volumes.
5. Disable generation of 8.3 names on all NTFS volumes used for FILESTREAM data storage by running the following command at a command prompt:

   ```
   FSUTIL BEHAVIOR SET DISABLE8DOT3 1
   ```

6. Disable last file access time tracking in NTFS volumes used for FILESTREAM data storage by running the following command at a command prompt.

   ```
   FSUTIL BEHAVIOR SET DISABLELASTACCESS 1
   ```

7. Disable antivirus software from scanning FILESTREAM volumes if it's not mandatory within your organization. If antivirus scanning is mandatory, then set the policies to not automatically delete offending files. Deleting of these files leads to corruption of your FILESTREAM enabled database.
8. To reduce disk fragmentation, ensure disk volumes used to store FILESTREAM data get formatted with a 64K allocation. The default NTFS allocation is 4K.
9. Disable Auto Shrink and Auto Close options on FILESTREAM enabled databases to avoid disk fragmentation and poor performance.

Enabling FILESTREAM

To properly use Integrity with your SQL Server installation, change the settings for SQL Server Configuration to allow for database upgrades.

NOTE You cannot enable FILESTREAM on a 32-bit version of SQL Server running on a 64-bit operating system. If you try, the following error message is displayed:

```
FILESTREAM is not supported on this instance of SQL Server.
```

FILESTREAM is not supported on versions of SQL Server earlier than SQL Server 2008 or an instance of SQL Server running under WOW. To enable FILESTREAM, upgrade the instance of SQL Server, or if running under WOW, install the 64-bit version of SQL Server 2008. For more information, see *http://msdn.microsoft.com/en-us/library/cc645923.aspx http://msdn.microsoft.com/en-us/library/cc645923.aspx*.

To enable FILESTREAM, see the Microsoft SQL Server documentation at *https://docs.microsoft.com/en-us/sql/relational-databases/blob/enable-and-configure-filestream?view=sql-server-ver15 https://docs.microsoft.com/en-us/sql/relational-databases/blob/enable-and-configure-filestream?view=sql-server-ver15*.

SECTION

Installing Full-Text Search for SQL Server

Full-Text and Semantic Extractions for Search (Full-Text Search) in SQL Server lets applications run full-text queries against character-based data in SQL Server tables. Integrity requires installation of this optional feature for your SQL Server environment.

Full-Text Search is an optional component of the SQL Server Database Engine. If you did not select this feature when you installed SQL Server, run SQL Server setup again to add it. This topic gives general steps to install Full-Text Search. For more information, see the Microsoft SQL Server documentation for your version of SQL Server.

To install Full-Text Search in SQL Server:

1. If you want to verify whether Full-Text Search is already installed, issue the following query in SQL Server:

   ```
   SELECT FULLTEXTSERVICEPROPERTY ('IsFulltextInstalled')
   ```

If Full-Text Search is installed, the result is 1. If it is not installed, the result is 0.

2. Run SQL Server setup.
3. Click **Installation** on the left pane.
4. Click **New SQL Server stand-alone installation** or **add features to an existing installation**.
5. Provide appropriate responses to the prompts depending on which path you selected.
6. Select **Full-Text and Semantic Extractions for Search**.
7. Continue to the end of the installation process.
8. After the installation completes, restart the following services:
   - SQL Server 20*XX* Configuration Manager
   - SQL Server Services
   - SQL Full-text Filter Daemon Launcher

SECTION

Setting IIS X-Frame-Options to Allow

The Integrity web interface requires that the X-Frame-Options setting in IIS be set to **Allow**. If this value is set to **Deny**, the Integrity web interface displays an error message that indicates the content cannot be displayed in a frame.

SECTION

Installing Integrity for the First Time

Before beginning the Integrity installation, complete and submit the Readiness Checklist to confirm that the hardware and software platform where Integrity gets installed meets the minimum requirements. If you have not completed the Readiness Checklist, see *Completing the Readiness Checklist* (page 59).

To use the Integrity setup program:

1. Log in as an administrator on the computer where you want to install Integrity.
2. Close all open applications before starting the installation.
3. Navigate to the Integrity folder within the folders containing the installation files and double-click **`ISS_Setup.exe`**.
4. Click **Start Setup**.
5. Fill out any required fields.
6. Under **Select Features to Install**, click **Main** to expand the window.
7. By default, Integrity installs to `C:\Program Files (x86)\PAS\Integrity\`. To select a different installation folder, click the ellipsis (**...**) and select the installation folder you want.
8. The **Optional Features** window displays several components. Select the components to install based on your configuration and deployment plans.

- **Web Server** - This component installs the web application. The Web Server requires you to install the Data Collector component on the same server. If you do not want to install the Web Server, clear the check box.
- **Data Collector** - The Data Collector component performs updates to the database on a predefined schedule. This service can be installed on multiple servers or computers, each performing independent updates to a central database.

9. Click **Next** to continue.
10. On the **License Agreement** window, read and agree to the terms of the license agreement, and then click **Install**.
11. If you have UAC enabled, click **Yes** to continue.
12. Click **Finish** to close the setup program.
13. Enable **CLR strict security**, if needed in your environment. For more information, see *Updating SQL Server CLR Strict Security and Cost Threshold Settings* (page 20).

SECTION

Using the Integrity Administration Utility

The Integrity installation includes the installation of an Administration Utility, which is used to perform a variety of administrative and configuration functions, such as validating the product license, user authentication, Internet Information Services (IIS), and database access. Run this utility on the server where Integrity is installed.

To start the Admin Utility:

1. Click Windows **Start > PAS**.
2. Right-click **Admin Utility** and then click **Run as administrator**.
3. If Application authentication mode is selected, you are prompted to log in. Specify your Integrity administrator user name and password, and then click **OK**.

Validating Your License

You license defines which functions are available for you and which asset models you can import and use. After you have installed Integrity, you need to validate your license.

The Licensing link in the Admin Utility opens the Product Licensing window. This window allows you to view your current license information and update your product license.

The Product Licensing window helps you validate your license, which you can complete by telephone or email. License validation is available 24 hours a day, seven days a week. Call or email Technical Support.

NOTES

- If your permanent Integrity license is in place, your current license information is displayed on the Product Licensing window.
- If Integrity is not currently licensed, you can click either **Begin** or **Send Email** to validate your license by telephone or email. For more information, see *Validating Your License by Telephone* (page 25) or *Validating Your License by Email* (page 25).

Validating Your License by Telephone

When you validate your license by telephone, you will provide a validation code to the PAS representative. Then, you will receive a permanent license file (`LicenseInfo.txt`) to add to your Integrity server.

To validate the license using telephone:

1. In the Admin Utility window, click the **Licensing** link.
2. Click **Begin**. Several windows help you complete the temporary license process.
   a. Click **I Agree** to accept the terms of the license agreement, and then click **Next** to see the telephone number to call PAS to validate the license.
   b. Click **Next**.
   c. After reading the code to the PAS representative, type the validation code in the field provided, and click Next.
   d. A confirmation is displayed when a valid code has been entered.
3. In the meantime, you receive an email from PAS that includes a permanent license file called `LicenseInfo.txt`.
   a. Save the `LicenseInfo.txt` file where you installed Integrity, typically `C:\Program Files (x86)\PAS\Integrity`.
   b. Close and reopen the Admin Utility before proceeding with Integrity configuration.

Validating Your License by Email

When you validate your license by email, you need to send a request for a license validation file to PAS. You will receive a reply from PAS, including two license files.

To validate the license using email:

1. In the Admin Utility window, click the **Licensing** link.
2. Click **Send Email**.
3. Click **I Agree** to accept the terms of the license agreement, and click **Next** to enter your Name, Company Name, Telephone Number, and Comments. Then click **Next**.
4. You may send the email in one of two ways. Follow the directions on the Send Email window to either send the email automatically, or you can send the email manually.
   a. On the Send Email window, click **Send Now** and the default email program sends the message automatically to PAS.
   b. If you choose to send the email manually, follow the instructions for composing the email.

   NOTE You need to attach the `IID.txt` file located in the installation folder if sending manually.
5. Click **Close**.
6. Technical Support sends an email that includes the `LicenseInfo.txt` and `LVC.txt` files.
   a. Save both files where you installed Integrity, `C:\Program Files (x86)\PAS\Integrity` by default.

b. In the Admin Utility window, click the **Licensing** link.

c. Follow the directions in the email from PAS to load the files.

d. Close and reopen the Admin Utility before proceeding with configuration.

SECTION

Managing Your Databases

During the installation process, you configure the Integrity database. This section provides the initial configuration and upgrade information, as well as other options that include enabling asset roll back and using multiple databases.

Creating the Database

After running the Integrity setup program and validating your license, you need to create and configure the database using the Admin Utility.

NOTE Attention Integrity customers who plan to upgrade to Experion PKS R430. Experion PKS R430 uses Microsoft SQL Server 2012 as its application database. On any Integrity Data Collector importing R430 data, SQL Server 2012 or later is required. If you have any questions or concerns, please contact Technical Support for assistance.

To create a new database:

1. In the Admin Utility, click the **Database** link.
2. Click **Yes** to specify that a new database will be created.
3. If you want a location other than the default location for the database files, specify the new location in the **Location** field. The default location depends on the Microsoft SQL Server installation location.
4. In the **Database Connection** area, indicate the Computer name (SQL Server name) and Database name. If the Microsoft SQL Server installation where the Integrity database will be located is a named instance, type the server name followed with a backslash and the instance name in the **Computer Name** field, such as `Server\Instance`.

   The database name must begin with a letter or underscore. Database names can contain only letters, numbers, underscores, dashes, and periods. No special characters can be used.
5. In the **Authentication** area, indicate whether Integrity should log in to Microsoft SQL Server using your Windows account or a specified SQL Server user ID and password. If you select **SQL Server mode**, type the user ID and password defined within SQL Server.

   NOTE For either authentication mode, the user account must be a member of the **dbcreator** (min) or **sysadmin** fixed server role and must be assigned to the **db_owner** database role. Use SQL Server Management Studio to assign the **db_owner** database role to the account you specify.
6. If you want to enable Integrity to support a large number of users, check the **Enable SQL Server managed session state** check box in the **Additional Configuration** section. The default setting is unchecked.
7. If you want to enable import roll back, check the **Enable Asset Roll Back** check box in the **Additional Configuration** section. Then, click **Yes** on the Confirm Creating Additional Database window.

Asset Roll Back allows administrators to roll back to a previously imported set of data in the event that the most recent import of data is old, invalid, or corrupted. For more information, see the *Administration Guide*.

8. Click **Save**.
9. Click **OK** on the Database Creation confirmation message window. The Database ID window is displayed.
10. If you want to use multiple databases, specify a unique ID number for the database. If this database is the only database, leave the value set to **1**. For more information, see *Configuring Multiple Databases* (page 27).
11. Click **OK** to close the Database ID window and create the database. When the process finishes creating the database, a confirmation message is displayed.
12. Click **OK** to close the confirmation window.
13. If a message is displayed that indicates the Integrity services must be restarted, complete the following steps:
    a. Click **OK** to close the restart services message window.
    b. Click the **Service Administration** link.
    c. In the **Select a Service** area, select **IntegrityDataCollector2**, and restart it.
    d. In the Select a Service area, select **PAS WebFileService**, and restart it.

Configuring Multiple Databases

Multiple databases allow you to segment larger amounts of data and view the consolidated data as needed. Each site can have a secondary database, and the centralized engineering group can have the primary database to view information across the databases. To use multiple databases, an administrator uses the Admin Utility to create the primary database with the database ID set to 1. Next, the administrator creates one or more additional, secondary databases with unique database IDs. Then, the administrator configures Integrity to recognize these databases and to coordinate data requests for assets stored in secondary databases.

To make sure the Integrity services and utilities work properly with multiple databases, the **pasIntegrityDB** and **IntegrityDataCollector2** services on the Integrity server for the primary database need to run using a domain account. This domain account allows the pasIntegrityDB service to see the assets in the secondary databases for multiple database services to perform correctly. You also need to modify the .config file for Integrity and each utility to identify the domain account you set up for the services to use. For more information, see *Defining Your Service Accounts* (page 32).

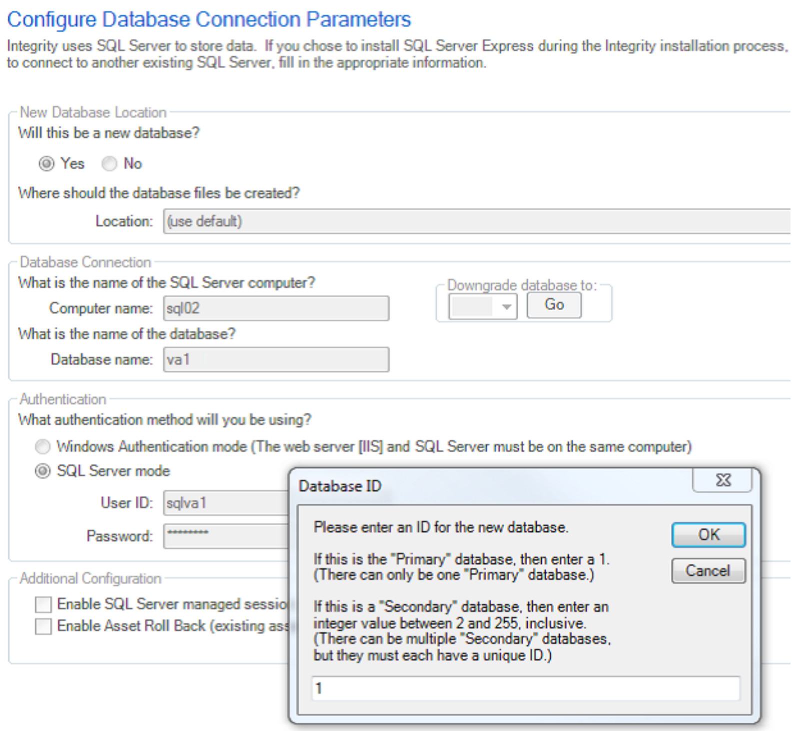
When you use multiple databases, some features, such as baselines, may require additional configuration and considerations for the primary database. For more information, see the *Integrity Administration Guide*.

NOTES

- If the password for the service and utilities account is changed in the future, you must also change the service configuration or the service will no longer work.
- The names of the assets across all databases must be unique.

To configure multiple databases:

1. Create one primary database using the Admin Utility and set the database ID to 1. Only one primary database can exist. For more information, see *Creating the Database* (page 26).



2. Create one or more secondary databases using the Admin Utility and set the database ID for each secondary database to a value other than 1. For a secondary database, the database ID can be an integer between 2 and 255, and the database ID must be unique.

3. Open the Integrity server for the primary database, which will be the web server, and then open the `IntegrityMOCRoot.XML` file in the folder where you installed Integrity, `C:\Program Files (x86)\PAS\Integrity` by default.

4. Copy the `<IMOCConnStr>` line, and then paste and rename the line as `<MainDB>` as shown in the following image.

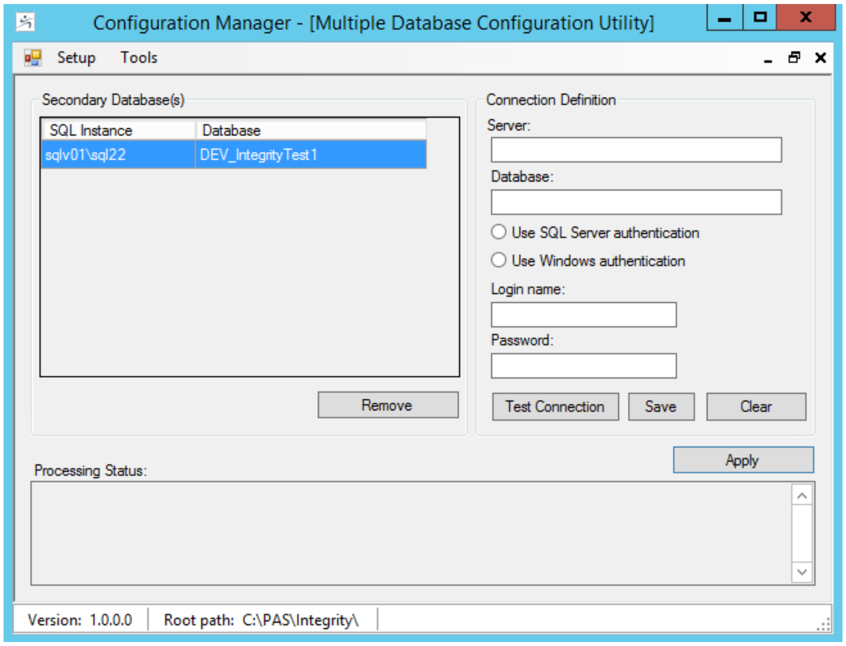
```
<?xml version="1.0" encoding="utf-16"?>
<IntegrityMOC>
  <IMOCConnStr>QiFsD5wLIZU4jMv8qjA7raD==</IMOCConnStr>
  <MainDB>QiFsD5wLIZU4jMv8qjA7raD==</MainDB>
  <IMOCAuthType>Windows</IMOCAuthType>
  <IMOCNoUserValidation>False</IMOCNoUserValidation>
```

5. In each secondary database, create the assets for that database using unique names across all databases. Then, import the data for each asset in each database.

6. Open Configuration Manager on the Integrity server for the primary database. To open Configuration Manager, run the following file:

   `InstallPath\DataCollector\ConfigurationManager.exe`

7. Click **Tools > Multiple Database Configuration**.



8. For each of the secondary databases, complete the following steps:
   a. Type the connection information for the secondary database, including server name, database name, authentication type, and login credentials.
   b. Click **Test Connection** to make sure the connection information is correct.
   c. Click **Save**.
9. Click **Apply**. Then, click **OK**. Integrity adds the data owners from the secondary databases to the primary database data owner table.
10. Close Configuration Manager.
11. Identify a domain account to use for the **pasIntegrityDB** service, **IntegrityDataCollector2** service, and the Integrity configuration utilities. For more information, see *Defining Your Service Accounts* (page 32).
12. On the Integrity server for the primary database, configure the services to use the domain account identified by completing the following steps:
    a. Click Windows **Start > Run**.
    b. Type `services.msc`, and then click **OK**.
    c. Right-click the **pasIntegrityDB** service, and then click **Properties**.
    d. Click the **Log On** tab, and then select the This account option. Type the domain account user name and password.

       NOTE If the password for this account is changed in the future, you must also change this specified value or the service will no longer work.
    e. Click **Apply**, and then click **OK**.
    f. If the service is not running, click **Start the service**.

g. Repeat these steps (**a-f**) for the **IntegrityDataCollector2** service.

13. Verify the **pasIntegrityDB** service has started correctly and is running by completing the following steps:

    a. Open the InstallPath\DataCollector\pasIntegrityDB.txt file, where InstallPath is the folder where you installed Integrity.

    NOTE If the pasIntegrityDB.txt file does not exist, the service never started.

    b. Verify no major errors exist.

14. On the Integrity server for the primary database, specify the identified domain user account in the `.config` files for Integrity and its configuration utilities by completing the following steps:

    a. Use Notepad to edit the following files:

    InstallPath\web.config

    InstallPath\DataCollector\AdminUtility.exe.config

    InstallPath\DataCollector\AMDK.exe.config

    InstallPath\DataCollector\AssetModelBuilder.exe.config

    InstallPath\DataCollector\IDC.exe.config

    InstallPath\DataCollector\
    IntegrityDataCollector2.exe.config

    InstallPath\DataCollector\WFSAlerts.exe.config

    b. Find the <userPrincipalName value=domain\username□/> tag in each file.

```
      </netNamedPipeBinding>
    </bindings>
    <client>
      <endpoint address="net.pipe://localhost/" binding="netNamedPipeBinding" bindingConfigurat
        <identity>
          <userPrincipalName value="domainname\username" />
        </identity>
      </endpoint>
    </client>
  </system.serviceModel>
</configuration>
```

    c. Change domain to the domain name of the primary Integrity server and change username to the domain account name associated with the **pasIntegrityDB** and **IntegrityDataCollector2** services.

    d. Save the files, and then close Notepad.

15. Open Configuration Manager on the Integrity server for the primary database. To open Configuration Manager, run the following file:

    InstallPath`\DataCollector\ConfigurationManager.exe`

16. Build the asset hierarchy so you can manage assets from secondary databases. You can drag and drop assets to Asset Explorer to define the hierarchy for Asset Explorer in the Integrity web interface, or you can use Microsoft Excel to specify your asset hierarchy, and then copy and paste that data to the object grid. For more information about defining your asset hierarchy, see the *Administration Guide*.

Importing Asset Models Using Multiple Databases

Certain core asset models need to be imported into specific databases to function correctly. For example, the Baselines asset model should be imported into the primary database. For more information, see the Administration Guide.

The source asset models, such as PAS Recon or Honeywell EPKS, should be imported into the appropriate secondary databases, where needed. For more information, see the Implementation Guide for each source asset type.

Defining the Web Application (Integrity Web Interface)

The Virtual Directory link in the Admin Utility is used to configure several options including the virtual directory for the Integrity web interface. The Admin Utility also allows you to restart the Integrity services and define trusted domain credentials.

To configure the Web application:

1. In the Admin Utility, click the **Virtual Directory** link. The Manage Virtual Directory Settings window for the version of IIS installed on the server is displayed.
2. Use the **Site Name** and **Port** fields to select a site and port for the Integrity web interface, or use the default web site and port 80.
3. In the **Application Name** field, type the name for the virtual directory to be used by IIS for user access to Integrity. This field defaults to **Integrity**. If Integrity is in multiple database mode, this field is unavailable and it must match the database name.
4. If you want to use a secure connection (HTTPS), check the **Use a Secure connection** check box and make sure IIS is set up for https support.
5. Note the URL for users to access Integrity. The URL is the server name and the virtual directory name, such as http://Server/VirtualDirectory.
6. Click **Yes** for the **Set permissions** option to grant the permissions necessary for the ASP.NET account to access the virtual directory.

   For Integrity to run properly, permissions must be granted to the virtual directory for the account under which IIS runs. This account is referred to as the ASP.NET worker process account. The name of the account used for running IIS must be entered into the ASP.NET worker process **Account name** field on the Manage Virtual Directory Settings window. If you select **No** for the **Set permissions** option, you are responsible for setting directory permissions appropriately.

   If your company security policies require that these accounts provided by the .NET Framework be disabled or deleted, you need to create another system account that has the following permissions:

   - Read and Write permission on the Integrity application (Integrity) folder.
   - Read and Write permissions on the Reports folder on the same level as the Integrity application folder. The Reports folder does not exist until a report is run from Integrity.
7. Click **Save**.

Defining Your Service Accounts

Integrity uses several services to provide various features. The **Service Administration link** in the Admin Utility displays the Configure the Services window. This window allows you to start and stop each service. You can also specify the account user name and password for each service to use. These services should run under valid domain accounts, and the permissions required for these accounts depend on whether you chose **Windows authentication mode** or **SQL Server mode** to access the Integrity database:

IntegrityDataCollector2

Provides data import and management capabilities. This service must run on each Integrity data collector or server where asset data is imported. The account you specify for this service must have access to the data to be imported into Integrity. This data can reside in files, folders, or databases, and can be located on computers other than the Integrity server or data collector. Because this service can run only as a single account, the various data locations must be configured to allow read access to this account. If Integrity imports SharePoint data via Document Manager, the account specified for this service must have permissions to access SharePoint and its data.

By default, this service runs under the SYSTEM account. If the Integrity data files, the Integrity database, and the Integrity server are all on the same server, and the service is running under Local System, you do not need to specify an account for this service on this window.

If the Integrity database is on a separate server and you chose **Windows authentication mode**, this service account must have the db_owner role on each primary and secondary database. When using multiple databases, if a secondary database is on a separate server from the primary database, this service account must also have the setupadmin role on the primary database to create a database link.

PASIntegrityDB

Provides data management for multiple database deployments. This service is not needed for single database deployments. When using multiple databases, this service must run on the Integrity server for the primary database. The account you specify for this service must be a valid domain account. In addition, you need to specify this account in the `InstallPath\DataCollector\*.exe.config` files on the Integrity server for the primary database.

PASWebFileService

Provides features for the Integrity web interface, such as email notifications and reporting capabilities. This service must run on the Integrity server that provides the Integrity web interface. Depending on your site security, the account you specify for this service could be a local user account or a domain user account and have read and write permissions to the folder where you installed Integrity and its subfolders. If you have specified a local user account and experience issues, specify a domain user account. For email notifications, this service uses the settings specified through **Maintenance > Configure Email Settings** in the Admin Utility.

PASWindowsEventLog

Provides Windows event log data processing and management. This service must run on each Integrity data collector or server where Windows event data is imported. The account you specify for this service must have read permissions to the folder where you installed Integrity. This account must also have read and write permissions to the folder and subfolders where event log data to import is stored. Integrity stores Windows event log data in a separate database named PASWindowsEventLogs.

If you collect Windows event log data, the account used to connect to the database (SQL login for **SQL Server mode** or the PASWindowsEventLog service account for **Windows authentication mode**) must have the following roles:

- dbcreator and serveradmin server roles
- If you chose Windows authentication mode, the PASWindowsEventLog service account must also have the db_owner role for the SQL Server where the Integrity database is stored and the db_datareader role for the Integrity database.

If you collect Windows event log data and if you chose **Windows authentication mode**, the administrator who uses the Admin Utility to create the Windows event log collection database must have at least the dbcreator role on the SQL Server where the Integrity database is stored.

PASIntegrityScheduler

Provides features for the Integrity web interface, such as email notifications and scheduled tasks. The first time you run the service, Integrity creates a new database (PASScheduler) on the Integrity data collector server.

This service is required in the following scenarios:

- Apply normalization rules as you modify or add them
- Manage impact factors and groups for Vulnerability Management

Ensure that the PASIntegrityScheduler service is running on the Integrity web server (the IIS server hosting the Integrity web interface). If the connection to the Integrity database is using **Windows authentication mode**, the PASIntegrityScheduler service needs to run as a domain account that has db_creator on the server and datareader on the Integrity database. If the connection to the Integrity database is using **SQL Server mode** for login authentication, the SQL Server login account used for the web interface needs the db_creator server role on the SQL Server instance.

PASIntegration

Provides features for the Integrity web interface, such as integrations with third-party applications. This service must run on the Integrity server that provides the Integrity web interface.

Review the following additional considerations for the account you specify for each service to use and related Windows accounts:

- If the Integrity database uses Windows authentication, these services can run as Local System only if the Integrity data files, the Integrity database, and the Integrity server are all on the same server.
- If the Integrity database uses Windows authentication, some of these services need to use accounts that have permissions to access the SQL Server database.
- For each account you specify, if the password for that account is changed, you must also change the password through the **Service Administration** link in the Admin Utility or through the service configuration itself.
- By default, SQL Server uses the NETWORK SERVICE Windows account for many functions. For example, the IntegrityAppPool for the Integrity web interface uses the NETWORK

SERVICE by default. Set the NT AUTHORITY/NETWORK SERVICE Windows account to have permissions to the Integrity database.

- Maintenance jobs require the SQL Server agent service to be active and running under a Windows account that has permissions to the Integrity database. Set the SQL Server agent service to run under the NT AUTHORITY/NETWORK SERVICE Windows account and to start automatically.

To specify the service accounts:

1. In the Admin Utility, click the **Service Administration** link.
2. In the **Service name** field, select the service to configure.
3. Type the user name and password for an account that has the required permissions for the service. Click **Get Accounts** to view all accounts on the server.
4. To preface the account name with the domain name and backslash, check the **Add Domain to Username** check box.
5. Click **Save**.

Setting Up the Asset for ICS Integrity Features

If you are installing and configuring ICS Integrity, you need to import the PAS Cyber Integrity asset model and create an asset using this model. Then, you can configure the specific ICS Integrity features you want to use. This section describes this initial ICS Integrity set up.

To import the PAS Cyber Integrity asset model and create the asset:

1. On the Admin Utility Welcome window, click the **Asset Models** link.
2. Click the **Browse** button to locate the model files provided by PAS, typically, `C:\Program Files (x86)\PAS\Integrity\DataCollector\Asset Models`.

   NOTE The Data Collector cannot access files on mapped drives. Use only Universal Naming Convention (UNC) paths.
3. From the **Available asset model(s)** list, click **PAS ICS Integrity** and then click the **[>]** button to move the asset model to the **Asset model(s) to be imported** list.

   The **Version** column indicates the availability of the asset model. If the model is listed as **Not Available**, you cannot add it to the **Asset models to be imported** list.
4. Click the **Import** button to import the files into Integrity.

   NOTE After importing an asset model, you can check the **MOC** section in the Windows Event Viewer to verify that no errors occurred during the import. When using multiple database mode, the Import button imports the model into all projects.
5. Add an asset for the PAS Cyber Integrity asset model by completing the following steps:
   a. On the Admin Utility window, click the **Asset Configuration** link.
   b. Click **Add** at the bottom of the list of assets.
   c. In the **Asset Name** field, type `CyberIntegrity`.
   d. In the **Asset model** field, select **PAS Cyber Integrity**, and then click **OK**.

Now that the PAS Cyber Integrity asset exists, you can configure ICS Integrity features you want to use. First, continue with the remaining sections of this guide to complete your Integrity installation and configuration. Then, you can add the ICS Integrity features you want:

- **Recon** to include Windows computer assets.
- **Vulnerability Management** and **Patch Management** for your assets.
- **Workflows** to use cases for change management and the integration with other features.
- **Baselines** to identify deviations from standard configurations.
- **Policies** to audit object properties against a desired standard.
- **Inventory** to search and browse inventory items for computers, network devices, and industrial control systems.
- **Event Analytics** to monitor critical Windows systems.
- **Topology** to provide Risk Analytics visualizations.

For more information about configuring these features, see the *Integrity Administration Guide*.

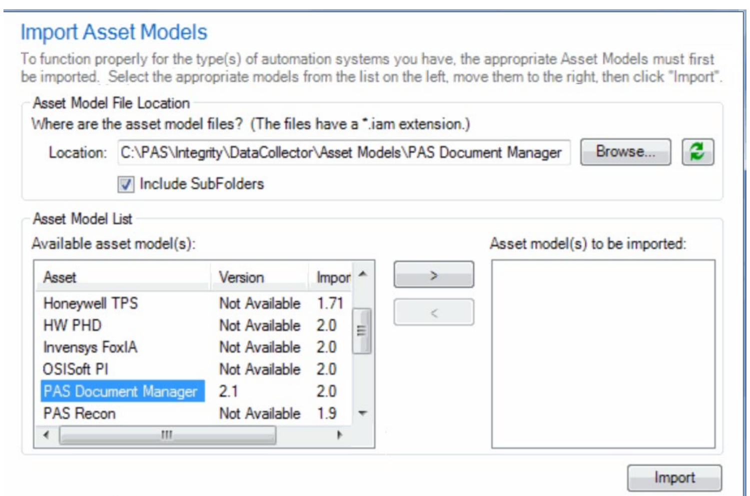
Loading (Importing) an Asset Model

An asset model provides information to Integrity about a specific class of systems, such as Honeywell EPKS or Yokogawa Centum VP. Integrity provides many asset models to support a wide range of systems. The **Asset Models** link on the Admin Utility window opens the Import Asset Models window. From this window, you can import one or more asset models that you have purchased.

To load an asset model:

1. On the Admin Utility, click the **Asset Models** link.
2. Click the **Browse** button to locate the model files provided by PAS, or type the path to the asset models to be loaded, such as `InstallPath\DataCollector\Asset Models`. The Data Collector cannot access files on mapped drives. Use only Universal Naming Convention (UNC) paths.
3. From the **Available asset model(s)** list, click on a model to load and then click the > button to move the asset model to the **Asset model(s) to be imported** list.

   NOTE The **Version** column indicates the availability of the asset model. If the asset model is listed as **Not Available**, you cannot add it to **Asset model(s) to be imported**.



4. Click the **Import** button. Integrity displays a message to confirm success.

> **NOTE** After you load an asset model, view the Windows event viewer to verify no errors occurred during the loading process.

To launch the Windows Event Viewer:

1. Click Windows **Start > Run**.
2. Type `eventvwr` then press Enter.
3. Click **IntegrityMOC** in the left pane to view the event log. Determine whether errors occurred from the time period associated with the asset model import.

Adding an Asset (Data Owner)

After you load an asset model, you can create one or more assets (data owners) for that type of system. The Asset Configuration link in the Admin Utility allows you to create new assets and configure the properties for existing assets. For more information about a type of system, see the Implementation Guide for the associated asset model, which provides detailed information and configuration instructions specific to that asset model.

The Asset Configuration link on the Admin Utility window allows you to create an asset for each system you want to import into Integrity. You need to import the asset model for the asset type and potentially perform other configuration tasks identified in the Implementation Guide for that asset model. Then, you can add the asset to Integrity and import data for that asset.

NOTE Before you add assets and schedule imports, see the Implementation Guide for each asset model you import. These guides provide information and instructions specific to each asset model type.

To add an asset:

1. In the Admin Utility, click the **Asset Configuration** link.
2. Click **Add**.
3. Type a unique name for the asset and select the asset model for this asset type.
4. Click **OK**.
5. Complete the following information depending on the asset model type:

   Import folder: Browse to or type the location of the files to import.

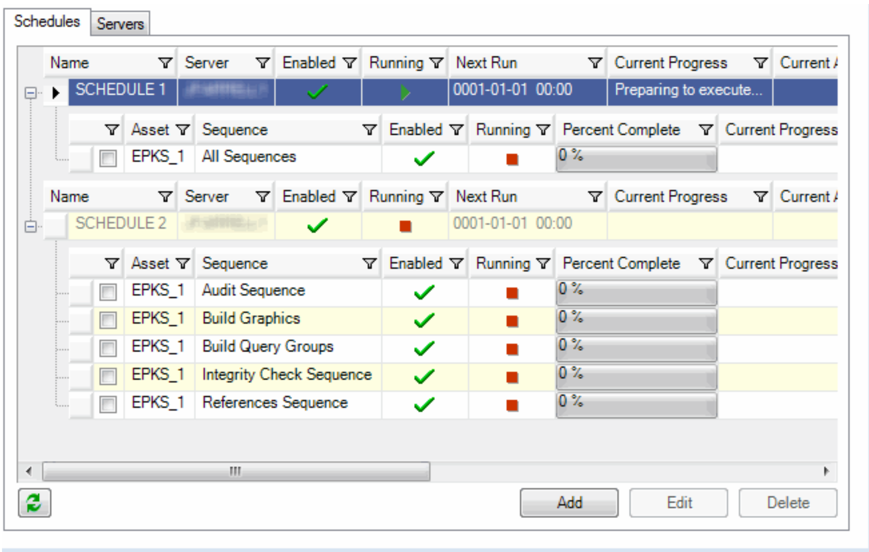
   Connection definitions: If information from outside data sources is required by this model, edit the connection to that data as needed.

   Asset properties: Edit properties specific to the asset model as needed as directed by the specific asset model Implementation Guide.
6. Click **Save**.

Scheduling Data Imports

After you have collected the data files from your systems, loaded the related asset models, and added the assets in Integrity, you can run or schedule a data import for those assets. For each asset, you need to direct Integrity to perform the data import and subsequent processing of the data. Typically, this procedure runs on a regular schedule that coincides with potential periodic updates in newly collected data.

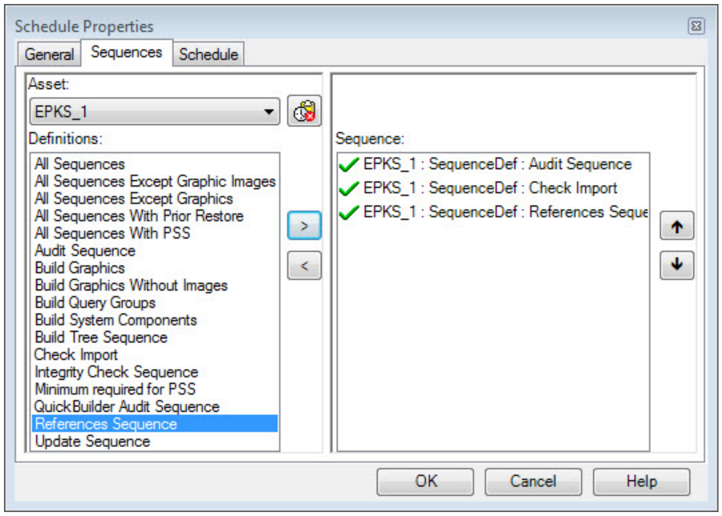
NOTE When you first install Integrity, you need to complete the data import process to make data available in the Integrity web interface. If you load a new version of an asset model, you may also need to complete the data import process for those type of assets to use the updated processing of the data defined by the asset model.



To import data now or on a scheduled basis:

1. In the Admin Utility, click the **Schedules** link.
2. Click **Add** to open the Schedule Properties window and add a new schedule.
3. Click **General** tab to name the import schedule and identify which Integrity server or data collector will import the data. Complete the following steps:
   a. In the **Schedule Name** field, type a descriptive name for the import schedule.
   b. In the **Server run on** field, type the name of the Integrity server or data collector that will import the data.
   c. If you want to disable the schedule, clear the **Enabled** check box. By default, this check box is selected so the import starts at the scheduled time.
4. Click on the **Sequences** tab to specify that data import tasks (sequences) and their order. This tab allows you to select sequence definitions for one or more assets in a single schedule. For each asset you want to include in this schedule, complete the following steps:
   a. In the **Asset** field, select an asset. To view a list of assets that have not been scheduled, you can click the **Schedule** button next to the **Asset** field.

b. In the **Definitions** list, select one or more sequences you want to run. Most asset models support an **All** sequence. Other sequences are available for testing and troubleshooting purposes, as well as for coordinating connected assets and cross references. In most cases, these other sequences should be used only when working with Technical Support. For more information, see the *Implementation Guide* for the associated asset model.



c. Click the **>** button to move the selected sequence to the **Sequence** list.

d. Use the up and down arrow buttons to adjust the order of the sequences. The tasks are run one at a time starting at the scheduled start time.

5. Click the **Schedule** tab to specify the frequency and start time for the import.
6. Click **OK**.

Monitoring an Import

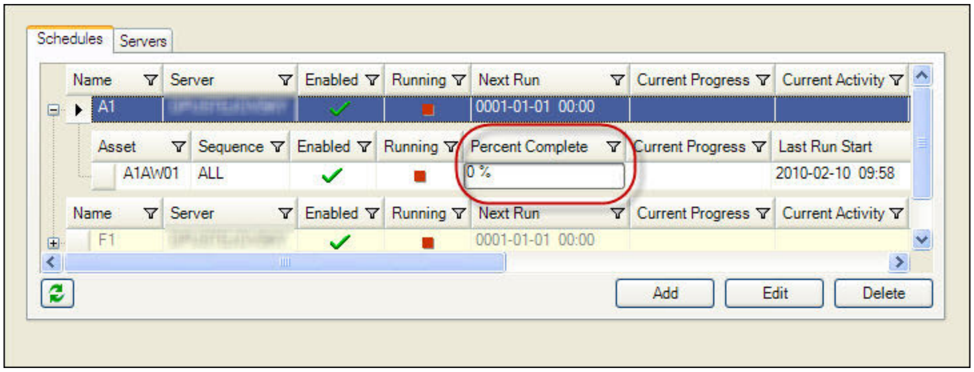
The **Schedules** link in the Admin Utility opens the Schedule Imports and Monitor Progress window. This window allows you to monitor the progress of an import and to view the import log, if needed. You can also view the history for a scheduled import.

Integrity also provides the Review a History of Imports window, which displays information concerning imported data for any asset model. Through the Review a History of Imports window, you can view more details about the imported data and roll back to a previous set of imported data if the database is configured to support data roll back. For more information about the history of data imports, see the Administration Guide.

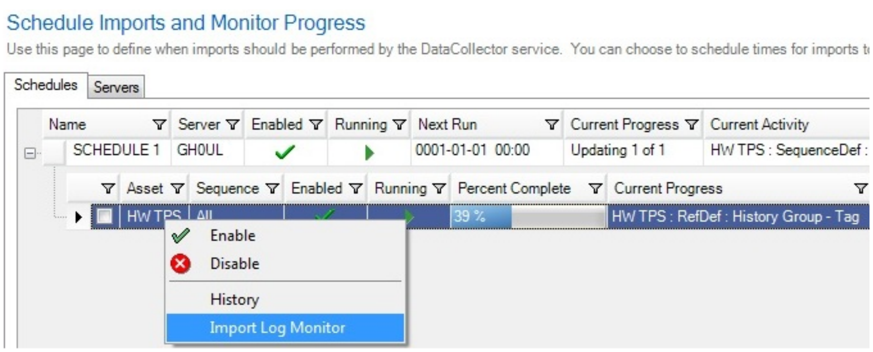
To monitor an import:

1. In the Admin Utility, click the **Schedules** link.

2. On the **Schedules** tab, click the plus sign (**+**) next to an import schedule to see the import tasks included in it. The **Percent Complete** column for each task provides progress information.



3. If you want to view the import log for a running import, right-click on an asset row, and select **Import Log Monitor**.



The Import Log Monitor window displays the contents of the import log, which you can scroll to view all the text. You can click **Refresh** to update the contents as the import progresses. To search the import log, type the criteria in the **Search for** field, and then click **Search**. The search text defaults to `exception` to search for errors in the log.

4. If you want to view the history of an import schedule, right-click on a scheduled import row in the Schedule Imports and Monitor Progress window, and select **History**. The Update Summary window is displayed with details about the imported data for the selected asset.

SECTION

Opening the Integrity Web Interface

The authentication process occurs each time users open the Integrity web interface or the Admin Utility. Integrity supports two modes of authentication that you specified during installation:

Application Authentication

When Application Authentication is selected, users are prompted to login with a user ID and password defined in the Admin Utility. If you have integrated the PAS Dashboard with the Integrity web interface, the PAS Dashboard also uses Windows pass-through authentication when displaying non-precalculated data. For more information, see the *PAS Dashboard User Guide*.

Windows Authentication

If Windows Authentication is used, users are not required to enter a user ID and password to open the Integrity web interface or Admin Utility.

To open the Integrity web interface:

1. In the URL Address field in a supported browser, type:

   `http://`*`ServerName`*`/`*`<VirtualDirectory>`*

   where *`ServerName`* is the name of the web server where Integrity is hosted, and <*`VirtualDirectory`*> is the name of the Virtual Directory created in the Admin Utility. For example, `http://Integrityserver/Integrity`.

   NOTE If you are using a secure connection, type https instead of http. If you do not know the Integrity web interface URL, you can open the Admin Utility, click the **Virtual Directory** link, copy the URL listed in that window, and paste that URL into the Address field of the browser.

2. If Application Authentication was selected during installation, type your Integrity user ID and password on the Login window, and then click **Login**.

If Integrity is configured to use Application Authentication, you can log out from the currently logged in user. To log out the currently logged in user from the Integrity web interface, click the **Log Out** link in the upper-right corner. This link is not available if Integrity is configured to use Windows Authentication.

SECTION

Additional Configuration and Troubleshooting Tasks

This section provides the following additional configuration tasks:

Setting Integrity Admin Utility to Always Run as an Administrator

The Admin Utility needs to run as an administrator.

1. Click the **Admin Utility** shortcut on the desktop.
2. Press Alt + Enter to display the Admin Utility Properties window.
3. On the Shortcut tab, Click **Advanced**.
4. Select the **Run as administrator** check box.
5. Click **OK** to close the Advanced Properties window.

6. Click **Apply**, and then click **OK** to close the Admin Utility Properties window.

Configuring Roles and Permissions in SQL Server

On the SQL Server computer, use SQL Server Management Studio to assign the required permissions:

- The person running the Integrity installation program needs to have at least the **dbcreator** role on the SQL Server where the Integrity database will be created. If using multiple databases, this person must have at least the **setup_admin** role.
- The IntegrityDataCollector2 service must run under an account with access to the database. If the Integrity database is on a separate server and you chose **Windows authentication mode**, this service account must have the **db_owner** role on each primary and secondary database. When using multiple databases, if a secondary database is on a separate server from the primary database, this service account must also have the **setupadmin** role on the primary database to create a database link.
- Integrity stores Windows event log data in a separate database. If you collect Windows event log data, the account used to connect to the database (SQL login for **SQL Server mode** or the PASWindowsEventLog service account for **Windows authentication mode**) must have the following roles:
  - **dbcreator** and **serveradmin** server roles
  - If you chose Windows authentication mode, the PASWindowsEventLog service account must also have the **db_owner** role for the SQL Server where the Integrity database is stored and the **db_datareader** role for the Integrity database.
- If you collect Windows event log data and if you chose **Windows authentication mode**, the administrator who uses the Admin Utility to create the Windows event log collection database must have at least the **dbcreator** role on the SQL Server where the Integrity database is stored.

To configure SQL Server login roles and permissions:

1. Click Windows **Start > Programs > Microsoft SQL Server 20*xx* > SQL Server Management Studio**.
2. Log in with the credentials provided by the site owner.
3. Expand the **Security** folder on the left.
4. Right-click **Logins** and then click **New Login**.
5. Select **SQL Server authentication** or **Windows authentication** as appropriate.
6. Select the appropriate roles for the authentication method you selected. For example, when using SQL Server authentication, you can select the **sysadmin** role in **Server Roles**, or you can select the **db_owner** role under **User Mapping** for each database used by Integrity.
7. Click **OK**.

Setting Up SQL Server Maintenance Jobs

Ensure you are using best practices to maintain all database servers in your Integrity installation. In most cases, the appropriate database administrator is responsible to maintain the database servers. This section provides the following configuration tasks related to SQL Server maintenance jobs recommended for your Integrity database servers:

Regarding Recovery Models for SQL Server

The Recovery Model used in this document for backup is the Simple Model. This is adequate for nearly all installations of Integrity. If there is a requirement for either a Bulk Logged or Full Recovery Model Backup plan, your SQL Server Database administrator would need to set up one of these plans.

For more information about the various Recovery Models, see *https://learn.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server?view=sql-server-ver16 https://learn.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server?view=sql-server-ver16*.

Checking for SQL Server Management Studio (SSMS)

Use SQL Server Management Studio as the administrative interface for SQL Server. You need to install SQL Server Management Studio when you install SQL Server on the computer. Occasionally, SSMS may not get initially installed. In such a case, you should install using the SQL Server installation media (CD or downloaded file). The existing SQL Server installation needs modification to include all components.

Checking for SQL Server Agent

Successful SQL Server maintenance jobs have the following requirements for the SQL Server Agent Service:

- Service must be active and running
- Service must run under a Windows user account that has the appropriate permissions to perform duties on the Integrity database and server.
- Ensure service runs under the Network Service (also known as NT Authority\Network Service) account,
- Service should be configured to start automatically.

To check these items:

1. Open Windows Services and select **SQL Server Agent** in the middle pane.
2. Click **More Actions > Properties** in the right pane.
3. Set the **Startup type** to **Automatic**.
4. Set the **Service status** to **Running**.
5. Click the **Log On** tab.
6. Set the account to **Network Service**. If not already set, click the **Browse** button, add **Network Service**, and click **OK**.
7. Click **OK** to close the SQL Server Agent Properties window.

Backup Database Configuration and Maintenance Plan

This section guides you through the process of creating the folder where backup files are stored and creating the Maintenance Plan to perform the backups.

To create a backup folder and maintenance plan to back up the database:

1. Enable Agent XPs. For more information, see *Agent XPs Server Configuration Option https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/agent-xps-server-configuration-option?view=sql-server-ver16* in Microsoft SQL Server documentation.
2. Create a folder on the SQL Server for storing the backup files named `Integrity_Backups`.
3. In the folder you created, create a subfolder named `Logs`.
4. Start SQL Server Management Studio.
5. Connect to the Database Engine using the credentials supplied on site.
6. Expand **Management** in the **Object Explorer w**indow in the left pane.
7. Right-click **Maintenance Plans** and click **Maintenance Plan Wizard**.
8. If an **Introduction** window is displayed, click **Next**.
9. Specify the following information on the **Select Plan Properties w**indow:

   Name: Type a name. For example, `Integrity`.

   Description: Type an optional description.

   Select **Single schedule for the entire plan** or **no schedule**.
10. Click **Change**.
11. On the **Job Schedule Properties** window, set the **Frequency**, **Daily frequency**, and **Duration** as appropriate, based on how often data imports occur (usually weekly). If possible, schedule the maintenance job for a period when no imports occur.
12. Click **OK** to close the **Job Schedule Properties** window.
13. Click **Next**.
14. On the **Select Maintenance Tasks** window, select **Back Up Database (Full)** and **Maintenance Cleanup Task**, and then click **Next**.
15. Use the **Move Up** or **Move Down** buttons to re-order the tasks so **Maintenance Cleanup Task** is first, and **Back Up Database (Full)** is second, and then click **Next**.
16. On the **Define Maintenance Cleanup Task** window, set the fields as follows:
    a. Under **Delete files of the following type**, click **Backup files**.
    b. Under **File location**, click **Search folder and delete files based on an extension**.
    c. In the **Folder** text box, type the path you created in Step 1, such as `D:\Integrity_Backups`.
    d. In the **File extension** text box, type `bak`.
    e. Select **Include first-level subfolders**.
    f. Under **File age**, select **Delete files based on the age of the file at task run time**.

g. In **Delete files older than the following**, set the time period based on how many backups you want to keep. For example, to keep four weekly backups, set the delete parameters to 4 weeks.

17. Click **Next**.
18. On the **Define Back Up Database (Full) Task** window, select the Integrity database in the list of databases, and then click **OK**.
19. On the **Destination** tab, select **Create a backup file for every database**, and then in the **Folder** text box, type the path to the backup location you created in Step 1, such as `D:\Integrity_Backups`.
20. Select **Create a sub-directory for each database**.
21. On the **Options** tab, change **Set backup compression to Compress backup**. All versions of SQL Server 2008 R2 or later have these options. Then click **Next.**
22. On the **Select Report Options** window, select **Write a report to a text file**.
23. In the **Folder location** text box, type the path for the logs you created in Step 2, such as `D:\Integrity_Backups\Logs`, and then click **Next**.
24. Click **Finish**, and then make sure the plan creates successfully.

Checking the Compatibility Level in SQL Server

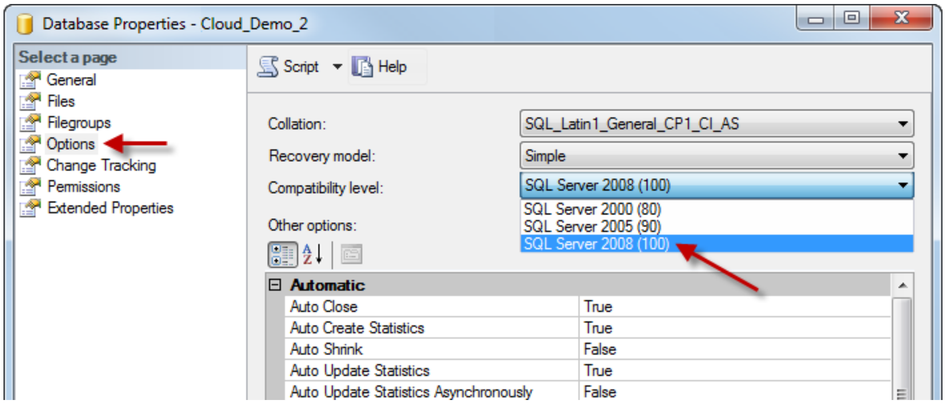
In Integrity, if the SQL Server database compatibility is set to SQL Server 2000 and below, the following error occurs:

```
Application Error:
System.Data.SqlClient.SqlException: Procedure or function
'IMOC_InsertMods' expects parameter '@Suppressed', which was not supplied.
The statement has been terminated.
   at PAS.DAL.SqlHelper.ExecuteNonQuery(SqlConnection connection,
CommandType commandType, String commandText, SqlParameter[]
commandParameters)
   at PAS.DAL.SqlHelper.ExecuteNonQuery(String connectionString,
CommandType commandType, String commandText, SqlParameter[]
commandParameters)
   at PAS.DAL.DataAccessLayer.mCmSaveImage(Guid ObjectID, String
PropertyName, Byte[] Image, Int64 Checksum, Boolean IsFile, String
UserName, enUpdateMethod UpdateMethod, String ApproversName, String
Reason, String StartTime, String DocType, Int32 PropertyAttribute)
   at PAS.AssetModeler.Propertee.Save(enUpdateMethod UpdateMethod)
End Application Error
```

To check database compatibility and prevent this problem:

1. Start SQL Server Management Studio.
2. Connect to the Database Engine using the credentials supplied.
3. Expand **Databases**, right-click the database, and then click **Properties**.
4. Select **Options** on the left.

5. Change the **Compatibility level** to the highest level available.



Performance Issues - Checking SQL Server Memory

In addition to ensuring the Integrity Server computer meets the requirements in the Readiness Checklist, Integrity requires a SQL Server database to store and process its data. To ensure optimum performance, you should properly configure the memory allocation of SQL Server.

Set the appropriate amount of memory to SQL Server. You should set 75% of memory for systems with 24 GB of RAM and above, or 50% of memory for system with below 24 GB or RAM.

To review and set the memory allocation:

1. Click Windows **Start > Programs > Microsoft SQL Server 20xx > SQL Server Management Studio**.
2. Connect to the Database Engine using the credentials supplied on site.
3. Right-click the instance at the top of the display, and then click **Properties**.
4. In the Server Properties window, select **Memory** in the left pane.
5. Change the Maximum server memory to the appropriate value in MB, and then click **OK**.

Issues with Report Generation for PDF or Visio

Integrity relies on the existence of the Desktop folder to properly create and save reports. If this folder does not exist in the proper location, reports may not be created correctly. If, when you click the Generate Report icon, it times out without creating a report, make sure the Desktop folder exists in the following path:

32-bit systems only have this one:

```
C:\Windows\System32\config\systemprofile\Desktop
```

64-bit systems display both of these:

```
C:\Windows\System32\config\systemprofile\Desktop
C:\Windows\SysWOW64\config\systemprofile\Desktop
```

If the folders do not exist, create the Desktop folder in those locations.

To ensure compatibility between Visio and Integrity, open any Visio file (*.vsd), and ensure that the file opens and is displayed correctly. When Visio launches the first time, it may display several windows requesting initial display settings and licenses. After you make sure that Visio opens files correctly, close Visio.

NOTE Visio 2003 and earlier do not include the PDF plug-in. You need to download the PDF plug-in for Visio for PDF printing to work. You might also need to install Adobe Reader on client machines that request PDF files from Integrity.

SECTION 3

Upgrading from a Previous Version

Before you install the new version, back up your database and configuration files. When upgrading from a version of Integrity prior to 7.3, you need to remove the previous version before you install the new version.

SECTION

Upgrading Integrity Steps

This section provides a list of the steps required to successfully upgrade Integrity. This list guides you through the other sections of this document.

1. Install the Full-Text and Semantic Extractions for Search feature in SQL Server if not already installed. This is an optional component of the SQL Server Database Engine. For more information, see *Installing Full-Text Search for SQL Server* (page 22).
2. Back up the current database and several configuration and licensing files. For more information, see *Backing Up the Database and Configuration Files* (page 48).
3. Record the group/user security permissions. For more information, see *Recording Group/User Names and Permissions* (page 48).
4. Stop the PASIntegrityScheduler service.
5. Uninstall Integrity. For more information, see *Uninstalling Integrity* (page 56).
6. Install the latest version of Integrity. For more information, see *Installing the Latest Version of Integrity* (page 48).
7. Validate your updated version license. For more information, see *Validating the Updated Product Version License* (page 49).
8. Upgrade your database, if needed. For more information, see *Upgrading the Database* (page 49).
9. Make sure to configure the Integrity services to run using appropriate accounts and start the services you need for your installation. For more information, see *Defining Your Service Accounts* (page 32).
10. Make sure the IntegrityAppPool application pool uses the latest .NET Framework. For more information, see *Set the Application Pool to Use .NET 4.8* (page 51).
11. Verify the Web application settings. For more information, see *Verifying Web Application Settings Following an Upgrade* (page 52).
12. If you are upgrading from a previous version that is using Vulnerability Management, upgrade Vulnerability Management settings. For more information, see *Upgrading Vulnerability Management* (page 52).
13. Review and consider any updated asset models. For more information, see Importing Updated Asset Models and *Scheduling Data Imports* (page 36).

14. Verify assets and asset details in Integrity. For more information, see *Verifying Upgrade Success* (page 56).

SECTION

Backing Up the Database and Configuration Files

Before continuing with the upgrade process, you should verify that you have a valid backup.

Make sure you have the latest copy of the following configuration files from the folder where Integrity is installed, typically C:\Program Files (x86)\PAS\Integrity:

- `IntegrityMOCRoot.xml`
- `LicenseIMOC.txt`
- `LicenseInfo.txt`
- `LVC.txt`

If you have an automated backup procedure, ensure that it has been running correctly and that the backup is current.

If you do not have an automated procedure, use Microsoft SQL Server Enterprise Manager or SQL Server Management Studio to make a backup. Instructions for performing a backup are described fully in the documentation for Microsoft SQL Server Enterprise Manager and SQL Server Management Studio. To verify the server name and/or database name, start the Administration Utility, and click **Database** to view the server and the database name.

SECTION

Recording Group/User Names and Permissions

If you install Integrity to a different location from the previous version, you might need to refer to previous security permissions details during the installation. Follow these steps to view current permissions.

To view Integrity security information:

1. From Windows Explorer or My Computer, navigate to the Integrity folder, typically `C:\Program Files(x86)\PAS\Integrity`.
2. Right click the Integrity folder and click **Properties**.
3. Click the **Security** tab.
4. Click each listed group or user to record the security permission information for each.

SECTION

Installing the Latest Version of Integrity

To install the latest version of Integrity, disable **CLR strict security** in SQL Server. For more information, see *Updating SQL Server CLR Strict Security and Cost Threshold Settings* (page 20). Next uninstall Integrity and then install Integrity as if installing it for the first time. For more information, see *Uninstalling Integrity* (page 56) and then *Installing Integrity* (page 12).

SECTION

Validating the Updated Product Version License

The Licensing link on the Admin Utility opens a window allowing you to view your current license information and/or update your product license. Since Integrity is already licensed, the current license information is displayed. License validation is available 24 hours a day, seven days a week. Call or email Technical Support. For more information about validating your license by telephone or email, see *Validating Your License* (page 24).

SECTION

Upgrading the Database

After completing the installation and validating your license, you need to upgrade the database to a newer version. The Database link on the Admin Utility main window opens the Configure Database Connection Parameters window. If your current database version is before Integrity 5.5, you first need to use SQL Server Management Studio to set the compatibility settings to at least SQL Server 2008.

NOTE Attention Integrity customers that plan to upgrade to Experion PKS R430. Experion PKS R430 uses Microsoft SQL Server 2012 as its application database. On any Integrity Data Collector importing R430 data, SQL Server 2012 or later is required. If you have any questions or concerns, please contact Technical Support for assistance.

To upgrade an Integrity database:

1. If your current database version is before Integrity 5.5, use SQL Server Management Studio to set the compatibility level settings to SQL Server 2008 (100) or higher. For more information, see *Checking the Compatibility Level in SQL Server* (page 44).
2. In the Admin Utility, click the **Database** link.
3. Click **No** to specify not to create a new database.
4. In the Database Connection area, indicate the **Computer Name** (SQL Server computer name) and **Database Name i**f not already available. If you reserved a copy of the IntegrityMOCRoot.xml configuration file from the previous installation and pasted it into the current installation folder, Computer name and Database name should display correctly.
5. In the Authentication area, indicate whether Integrity should login to Microsoft SQL Server using a Windows account or the specified user ID and password. If you select the latter option, enter a user ID and password.
    a. **For SQL Server Authentication**, use SQL Server Management Studio to assign the db_owner user role (e.g. the domain account name). Use this domain account name to access the database.
    b. Change the connection string displayed in the setup to read as follows:

    ```
    Computer Name=machine; database=;
    Authentication=SQL Server or Windows;
    User ID=user; password=pass;
    ```

    where `machine` is the computer name where the SQL Server is running; `user` is the SQL Server account name configured in the previous step; and `pass` is the password for that SQL Server user account.

c. For Windows Authentication, use SQL Server Management Studio and assign the db_owner user role for the database to the domain account to use to access the database. By default, the IntegrityDataCollector2 service runs under the SYSTEM account.

NOTE If Microsoft SQL Server is installed as a named instance, follow the remote server name with a backslash and the instance name (for example, Server1\Instance1).

6. Click **Save**. A Database Upgrade message window is displayed.

   NOTE The database upgrade to Integrity 7.3 may take over 30 minutes.

7. Click **Yes** on the Database Upgrade confirmation message window to upgrade the database structure to the latest version. Depending on the size of the database, this process may take anywhere from a couple of minutes to an hour or more. A message is displayed when the upgrade completes.

   NOTE If you made changes to the database settings, a message is displayed on the Admin Utility window indicating you should stop and restart the services.

8. Enable **CLR strict security**, if needed in your environment. For more information, see *Updating SQL Server CLR Strict Security and Cost Threshold Settings* (page 20).

Upgrading When Using Multiple Databases

After completing the installation and validating your license, you need to upgrade the database to a newer version. The Database link on the Admin Utility main window opens the Configure Database Connection Parameters window. You use Admin Utility to upgrade the primary database, and you use Configuration Manager to upgrade the secondary databases. If your current database version is before Integrity 5.5, you first need to use SQL Server Management Studio to set the compatibility settings to at least SQL Server 2008.

NOTE The steps for upgrading multiple databases may differ based on how your site is configured, however you should always upgrade your primary database first. If you have any questions or concerns, please contact Technical Support for assistance.

To upgrade the primary database:

1. If the current database version is before Integrity 5.5, use SQL Server Management Studio to set the compatibility level settings to SQL Server 2008 (100) or higher. For more information, see *Checking the Compatibility Level in SQL Server* (page 44).
2. Open Admin Utility and click the **Database** link.
3. Click **No** to specify not to create a new database.
4. In the **Database Connection** area, indicate the **Computer Name** (SQL Server computer name) and the primary database in the **Database Name** field if not already available. If you reserved a copy of the IntegrityMOCRoot.xml configuration file from the previous installation and pasted it into the current installation folder, Computer name and Database name should display correctly
5. In the **Authentication** area, indicate whether Integrity should login to Microsoft SQL Server using a Windows account or the specified user ID and password.
6. Click **Save**. A Database Upgrade confirmation message window is displayed.

   NOTE The database upgrade to Integrity 7.3 may take over 30 minutes.

7. Click **Yes** on the Database Upgrade confirmation message window to upgrade the database structure to the latest version. Depending on the size of the database, this process may take

anywhere from a couple of minutes to an hour or more. A message is displayed when the upgrade completes.

NOTE If you made changes to the database settings, a message is displayed on the Admin Utility window indicating you should stop and restart the services.

8. Enable **CLR strict security**, if needed in your environment. For more information, see *Updating SQL Server CLR Strict Security and Cost Threshold Settings* (page 20).

To upgrade secondary databases:

1. Open Configuration Manager on the Integrity server for the primary database. To open Configuration Manager, run the following file:

   InstallPath\DataCollector\ConfigurationManager.exe

2. Click **Tools > Multiple Database Configuration**.
3. For each of the secondary databases, complete the following steps:
   a. Under **Connection Definition**, type the connection information for the secondary database, including server name, database name, authentication type, and login credentials.
   b. Click **Test Connection** to make sure the connection information is correct.
   c. Click https://hexagonppm-uat.fluidtopics.net/r/en-US/Writer-s-Hub/Questions/312714?tocId=fYiTdk8Su~UZ6WwjRICrrA.
4. Click **Apply**, and then click **OK**.
5. Close Configuration Manager.

SECTION

Set the Application Pool to Use .NET 4.8

If upgrading Integrity, the existing IntegrityAppPool application pool may be using an older version of the .NET Framework. Make sure the IntegrityAppPool application pool uses the latest .NET Framework version.

To change the .NET Framework version for the application pool:

1. Click Windows **Start > Run**.
2. Type `inetmgr` and click **OK** to start IIS Manager.
3. Expand the server account on the left, and then select **Application Pools**.
4. Click **IntegrityAppPool**, and click **Basic Settings** in the right pane.
5. Choose .NET Framework v4.0x from the list, and then click **OK**.

   NOTE .NET Framework version 4.5 or later display as v4.0 in the list.

6. Click **File > Save** Connections.
7. Click **File > Exit** to close Internet Information Services (IIS) Manager.

SECTION

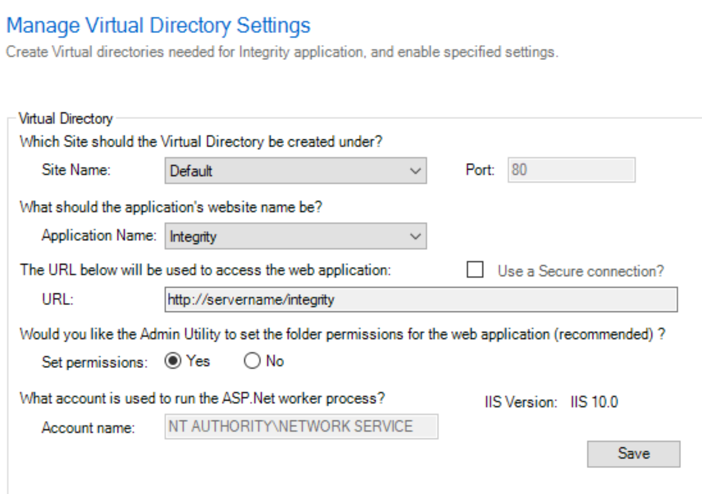
Verifying Web Application Settings Following an Upgrade

The Virtual Directory link on the Admin Utility window opens the Manage Virtual Directory Settings window.

NOTE Although configured during the initial Integrity installation, verify the Web application settings following an upgrade. This information should be accurate if you saved a copy of the `IntegrityMOCRoot.xml` configuration file from the previous installation and pasted it into the current installation folder.

To configure the Web application:

1. On the Admin Utility, click **Virtual Directory**. The Manage Virtual Directory Settings window for the version of IIS installed on the server is displayed.



2. Enter the name of the virtual directory used by IIS for access to Integrity.
3. Click **Yes** for the **Set permissions** option to configure the permissions necessary for the Network Service account to access the virtual directory.
4. Click **Save**.

SECTION

Upgrading Vulnerability Management

If you are upgrading from a previous version that is using Vulnerability Management, you must follow these steps to upgrade Integrity and Vulnerability Management:

1. Upgrade Integrity using the appropriate steps in the *Installation Guide*.
2. Import the latest Patch Management model. For more information, see the *Administration Guide*.
3. Schedule automated updates for the model and run the scheduled import.
4. Import the latest Vulnerability Management model.

NOTE If you are using the Patch Management and Vulnerability Management asset models, you must point to the following folder on the SFTP site for daily updates:

`PASVulnerabilityMgt_3_1`

5. Import the latest PAS Inventory Items asset model.
6. Schedule the inventory import to run following each import of data you want in vulnerability matching, such as Recon and TPS data.
7. Import the PAS Cyber Integrity asset model and create an asset using this model.
8. Schedule automated updates for the Cyber Integrity model, including the NVD Update Inventory Items schedule, and run the scheduled import.
9. Install and configure the PAS Dashboard using the steps in the *PAS Dashboard User Guide*. After installation is complete, complete the following additional steps using the PAS Dashboard Configuration program:
   a. Ensure the license is up to date.
   b. Connect to the Integrity database.
   c. Import the latest PAS Dashboard asset model.
   d. Click **Next** during each step in the Dashboard setup wizard.
   e. On step 6 of the wizard, click **Clear Compiler Output**, and then click **Restart Dashboard**.
   f. Restart IIS.
10. In Integrity, navigate to the ICS Integrity web interface and click **Vulnerability > Summary**.

    IMPORTANT Wait for the page to load, which could take minutes while the widgets recalculate.

If this is the first time that Vulnerability Summary has been opened since the upgrade process, the widgets will automatically populate within a minute.If the widgets do not repopulate or the web page has been previously opened and navigated away from before the page loaded, the widgets will not recalculate automatically unless new data has been imported. To recalculate the widgets, go to the Dashboard configuration web page at `http://`*`server`*`/dashboard/configure.aspx` and click **View screen > Vulnerability Summary > Recalculate**.

SECTION

Importing Updated Asset Models

An asset model provides information to Integrity about a specific class of systems, such as Honeywell EPKS or Yokogawa Centum VP. Integrity provides many asset models to support a wide range of systems. Integrity also provides asset models for other types of assets, such as PAS Recon for Windows computers and PAS Network Devices for network switches and firewalls. New versions of these asset models may be released between Integrity releases and you can import these asset models as needed.

Product Models

Some asset models, referred to as product models, provide additional product features. If you are using these asset models, you should import the latest version of the following asset models when you upgrade Integrity:

- PAS Compliance - NERC CIP (for Cyber Integrity)
- PAS Cyber Integrity (for Cyber Integrity)
- PAS Document Manager
- PAS Generic File Manager
- PAS Inventory Items
- PAS Policies (for Cyber Integrity)
- PAS Sensor Data Integrity

NOTE When you initially configure vulnerability and patch management, you automate the download and import of the latest PAS Vulnerability Management and PAS Patch Management asset models. Therefore, you do not need to manually import the latest version of these two asset models when you upgrade Integrity.

Customer Models

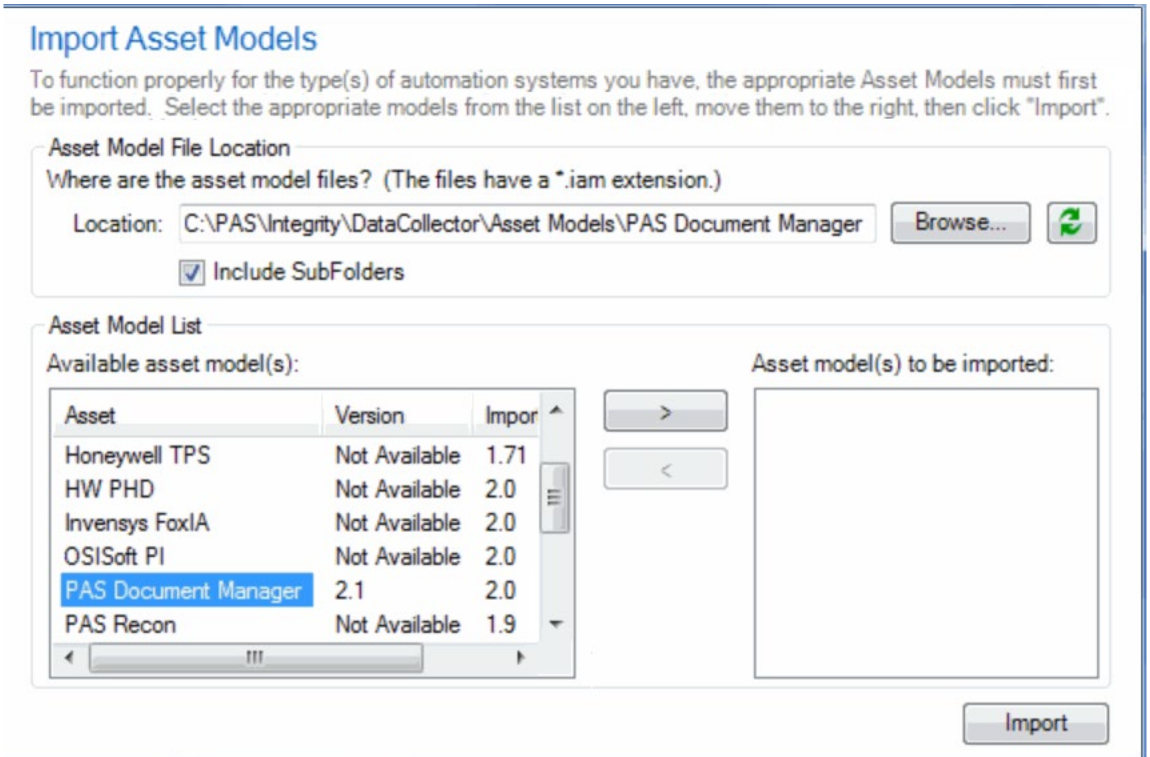
A few asset models, referred to as customer models, provide features that can include customer-specific implementation details. Many of these asset models have file names with square brackets. If you import an updated version of these asset models, you can lose some of your implementation settings. When a new version of the following asset models is available, contact Technical Support to determine how to adjust your model:

- PAS Maintenance
- PAS Workflows
- [PAS Baselines]
- [PAS Dashboard]
- [PAS Integration]

The **Asset models** link on the Admin Utility window opens the Import Asset Models window, which allows you to import updated asset models that you have purchased. The **Available asset model(s)** list provides several columns to help you determine which asset models you have and what version is available:

- **Version**: Indicates the availability of the asset model and what version is provided in the location specified in the **Location** field.

- **Imported**: Indicates the version of any previously imported asset model.



To import asset models:

1. On the Admin Utility - Welcome window, click **Asset Models**.
2. Click **Browse** to locate the model files provided by PAS, or type the path to the asset models to import, such as `InstallPath\DataCollector\Asset Models`.

   NOTE The Data Collector cannot access files on mapped drives. Use only Universal Naming Convention (UNC) paths.

3. In the **Available asset model(s)** list, click a model to import, and then click the [**>**] button to move the asset model to the **Asset model(s) to be imported** list.

   NOTE Do not import the customer models previously listed, such as PAS Workflow and [PAS Baselines]. Importing PAS Workflow through the Admin Utility removes your workflow implementations. Contact Technical Support to guide you through the process of importing the new model, if needed, and maintaining your implementation settings.

4. Click the **Import** button to import the files into Integrity.

   NOTE After importing an asset model, check the MOC section in the Windows Event Viewer to verify that no errors occurred during the import. When using multiple database mode, clicking the Import button imports the model into all projects.

To launch the Windows Event Viewer:

1. Click the Windows **Start** button, type **Run**, then press **Enter**.
2. Type **eventvwr** then press **Enter**.

3. In the left pane, expand **Applications and Services Logs**, and click **IntegrityMOC** to view the event log. Determine whether errors occurred from the time period associated with the asset model import.

SECTION

Verifying Upgrade Success

After upgrading to the current version, you should launch Integrity and confirm that all available information is displayed as in the previous version. For a detailed list of enhancements and fixes included in the upgrade, see the *Integrity Release Notes*.

To verify asset data in the latest version:

1. From the Integrity Dashboard, click **Explore**.
2. From the Asset Explorer, click the plus (**+**) sign next to each top-level asset.
3. Click various assets and verify that data is displayed correctly.

SECTION

Uninstalling Integrity

Uninstalling Integrity does not usually remove all user data. If you want to uninstall Integrity and do not intend to reinstall it, you need to manually remove the Integrity database on the Microsoft SQL Server computer. Before uninstalling Integrity, back up all your data and stop the data collector.

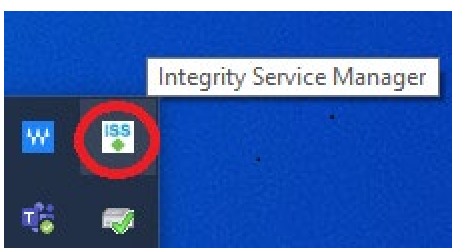
NOTES

- The uninstall process attempts to delete all installation files in the installation folder and all subfolders created during the installation process. Any files added to those folders after the installation will not be deleted. If users have manually stored files in subfolders in the installation folder, back up these files before beginning this process.
- If you uninstall Integrity with the intention of reinstalling or upgrading it, copy the license and configuration files (`LicenseInfo.txt`, `LicenseIMOC.txt`, and `IntegrityMOCRoot.xml`) from the default installation folder to another location before you remove Integrity. For more information, see *Backing Up the Database and Configuration Files* (page 48).

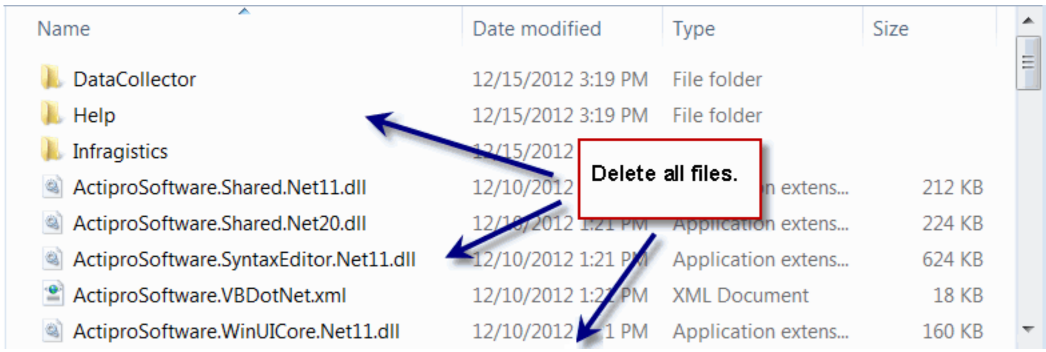
Integrity 7.2 or earlier

To stop the data collector and then remove Integrity 7.2 or earlier:

1. Right click the IntegrityServiceManager icon in the Windows system tray, and then click **Stop** to stop the data collector.



2. Click Windows **Start > Control Panel**.
3. Click the **Programs and Features** option (in the Programs category).
4. From the **Currently installed programs** list, click **Integrity** and then click **Change**.
5. After the uninstall process is complete, use IIS Manager to remove the Integrity and igcommon virtual directories.
6. After uninstalling Integrity, browse to the Integrity installation folder and manually delete any files and folders that did not delete during the uninstall process.



Integrity 7.3 or later

To stop the data collector and then remove Integrity 7.3 or later:

1. Right click the IntegrityServiceManager icon in the Windows system tray, and then click **Stop** to stop the data collector.
2. Navigate to the Integrity folder in the installation files, and double-click **`ISS_Setup.exe`**.
3. Select **Uninstall** from the list of options, and then click **Next**.
4. Click **Yes** to uninstall Integrity.
5. After the uninstall process is complete, use IIS Manager to remove the Integrity and igcommon virtual directories.
6. After uninstalling Integrity, browse to the Integrity installation folder and manually delete any files and folders that did not delete during the uninstall process.

Verify the Data Collector Was Removed

The uninstall process should remove the **IntegrityDataCollector2.exe**. The following task allows you to verify that it no longer exists and to manually remove it if needed.

To verify **IntegrityDataCollector2** uninstalled correctly:

1. Click Windows **Start > Run**.
2. Type `services.msc`.
3. Click **OK**.
4. Verify **IntegrityDataCollector2** no longer displays in the list.
5. If **IntegrityDataCollector2** still displays in the list, complete the following steps:
   a. Click Windows **Start > Run**.

b. Type `CMD` then press **Enter**.

c. Type the following at the command prompt:

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil -U
"InstallPath\DataCollector\IntegrityDataCollector2.exe"
```

where *InstallPath* is where you installed Integrity, typically `C:\Program Files(86)\PAS\Integrity`.

6. Complete the preceding steps again to verify the **IntegrityDataCollector2** no longer displays in the list on the **Services** window. If **IntegrityDataCollector2** still displays in the list, type in the following command at the command prompt:

```
sc delete IntegrityDataCollector2
```

SECTION 4

Completing the Readiness Checklist

The flexibility of Integrity allows you to deploy in many ways, depending on your network architecture, firewalls, and security policies. This section includes separate requirements for consolidated and dispersed implementations.

To prepare for Integrity:

1. Review the various deployment options. For more information, see Understanding the Deployment Options.
2. Consider the system requirements based on your selected deployment:

   Integrity Server System Requirements (page 65)

   Integrity Virtualization Requirements (page 80)

   Integrity Client Requirements (page 82)

   NOTE The number and types of asset models included with the installation determine the actual system requirements.
3. Integrity has no requirements for Transport Layer Security (TLS) protocols. If you choose to use TLS protocol, you can use the TLS protocol supported on the operating system and SQL Server version you use for Integrity.
4. Complete the checklist based on your intended Integritydeployment and send it to your technical contact. For more information, see *Readiness Checklist* (page 59).

Readiness Checklist

This checklist summarizes the information needed to install and configure Integrity. Please print this checklist, complete the information, and fax or email it to our Operations team.

To: Operations (operations@pas.com)

Telephone: +1 281.286.6565

Fax: +1 281.286.6767

Email: *operations@pas.com mailto:Operations@PAS.com*

From: ____

Site: ____

Email: ____

Telephone: ____

Fax: ____

Date: ____

Installation Size and SQL Server Sharing

1. Which is your installation size? For more information, see *Integrity Server System Requirements* (page 65).
   - Size A: ______
   - Size B: ______
   - Size C: ______
2. Are the Data Collector and the SQL Server computer shared? This option is available only for installation sizes A and B.
   - Yes: ______ (complete Item 2a.)
   - No: ______ (complete Item 2b.)

Attention Integrity customers who plan to upgrade to Experion PKS R430: Experion PKS R430 uses Microsoft SQL Server 2012 as its application database. The Microsoft SQL Server that serves Integrity should also be upgraded to Microsoft SQL Server 2012.

Shared Data Collector/SQL Server Computer Requirements

2a. Complete this item only if the Integrity Server and SQL Server are shared.

- Computer name: ______________________________ (cannot contain underscores)
- Domain name: ______________________________
- CPU: ______________ GHz
- RAM: ______________ GB
- Hard drive: ______________ GB
- Network Card 1 Speed: 10 / 100 / 1000
- Network Card 2 Speed: 10 / 100 / 1000 (if applicable)
- Network Card 3 Speed: 10 / 100 / 1000 (if applicable)
- Windows Version & Service Pack: ____
- Microsoft SQL Server Version: ____

Data Collector Server and SQL Server Computer Requirements

2b. Complete this item only if the Server and SQL Server are not shared.

Data Collector Server Requirements

- Computer name: ______________________________ (cannot contain underscores)
- Domain name: ______________________________
- CPU: ______________ GHz
- RAM: ______________ GB

- Hard drive: ______________ GB
- Network Card 1 Speed: 10 / 100 / 1000
- Network Card 2 Speed: 10 / 100 / 1000 (if applicable)
- Network Card 3 Speed: 10 / 100 / 1000 (if applicable)
- Windows Version & Service Pack: ____

SQL Server Computer Requirements

- Computer name: ______________________________
- Domain name: ______________________________
- CPU: ______________ GHz
- RAM: ______________ GB
- Hard drive: ______________ GB
- Network Card Speed: 10 / 100 / 1000
- Windows Version & Service Pack: ____

Integrity Login Account and Permissions

Integrity requires the following accounts and permissions:

- The server runs the **IntegrityDataCollector2** and **PASWebFileService** service. These services need a domain or common work group login account.
- The service account should have administrative permissions on the server.
- Initially, an account that can create databases in SQL Server is required.
- At a minimum, the account connecting to the SQL Server should have **Read**, **Write**, and **db_owner** permissions to the database (and ASPState database if configured).

Please answer the following questions:

- Domain account exists for the Integrity services?: Yes: ______ No: ______
- Domain account is added to the server local Administrators group? Yes: ______ No: ______
- Domain account has access rights to the database on the SQL Server? Yes: ______ No: ______
- On the day of installation, an authorized person with knowledge of the login and password for this account will be available? Yes: ______ No: ______

Firewall and Virus Scan Software

Firewall

If a firewall exists in your network architecture, the following unidirectional firewall rules need to be implemented. For more information, see Understanding the Deployment Options.

From Integrity components to the SQL Server:

- TCP port 1433

- UDP port 1434

From Integrity clients to the Web Server:

- Browser requires HTTP (usually port 80)

Virus Scan Software

Antivirus software type and version: ____

Internet Information Server (IIS)

IIS 7.0 or later is required on the Integrity Server and should be accessible from client computers.

To test whether IIS is installed and configured on the Integrity Web Server:

1. On the Integrity server, open the browser (Chrome, Chromium-based Edge, or Internet Explorer 11).
2. In the **Address** field, type `http://localhost` then press **Enter**. The default web page for IIS should be displayed.

To test whether IIS is accessible from a client computer:

1. On the client (any computer on the network where the client may be potentially installed), open the browser (Chrome, Chromium-based Edge, or Internet Explorer 11).
2. In the **Address** field, type `http://`*`IntegrityServer`* where *IntegrityServer* is the name of the Web Server computer, then press **Enter**. The default web page for IIS should be displayed.

Please answer the following questions:

- Is IIS 7.0 or later installed on the Integrity Server? Yes: ______ No: ______
- Is ASP.NET Framework 4.8 enabled? Yes: ______ No: ______
- Did you view the default IIS web page from the server? Yes: ______ No: ______
- Did you view the default IIS web page from a client computer? Yes: ______ No: ______
- Is IIS 7.0 or later installed on the Integrity Data Collectors? Yes: ______ No: ______

NOTE To access a Web Server through a firewall, the firewall should have the HTTP port open.

Email and Assets

Email

Please answer the following questions:

- Will Integrity be set up to send email notifications and links to reports?
  Yes: ______ No: ______
- What is the domain name of the email server?
  ____
- What is the name of the email server? ____________________________________

- What is the email server type (Exchange, Lotus Notes, Lync, for example)?
  ____

NOTE To send email through a firewall, the firewall should have the SMTP port open.

Assets

Please answer the following questions:

- With what types of control systems will Integrity interface?
  ____
- Are systems compliant with all requirements in the readiness checklist for each asset type supported? Yes: ______ No: ______

Signature for Checklist Sections

I have verified the previously listed items and certify that all requirements have been satisfied.

Signature: ____

Printed Name: ____

Date: ____

Telephone: ____

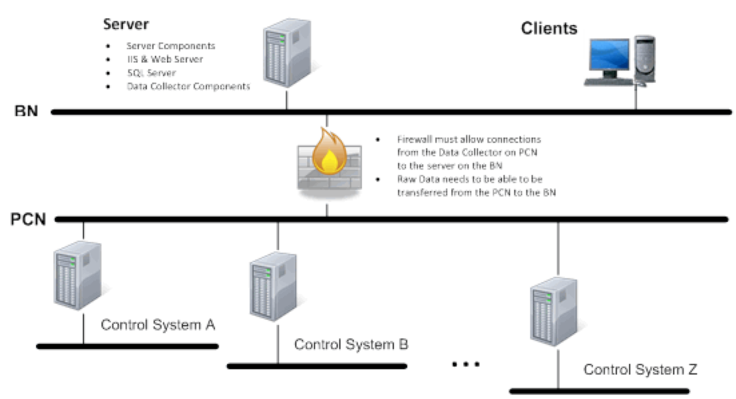
If you are not able to meet any of the previously listed requirements, or if you have any questions, contact Technical Support.

Understanding the Deployment Options

The following sections illustrate examples of Integrity deployment options. These examples are by no means the complete range of options. Integrity is very flexible and can be deployed in many different ways, depending on network architecture, firewalls, and security policies. Work with your PAS contact to establish the deployment configuration most suitable to your site.

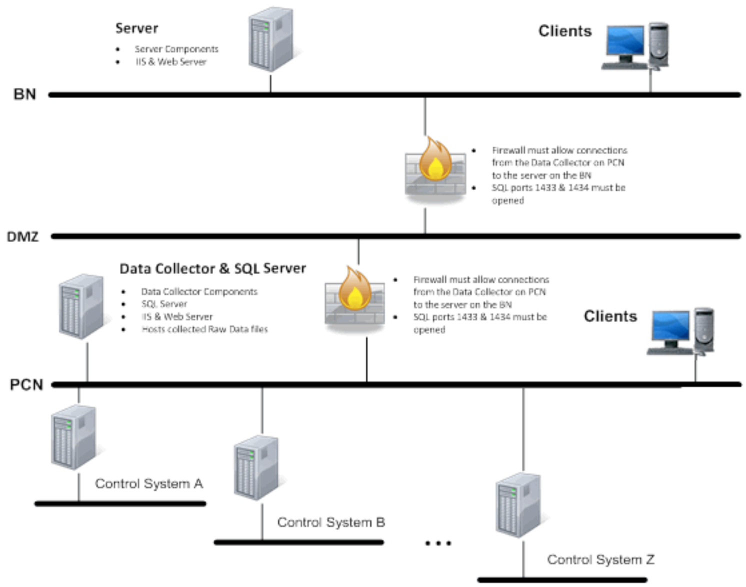
Multiple Data Collectors, which are recommended for medium and large sites, can be used with any of these options.

Typical Dual Network Deployment



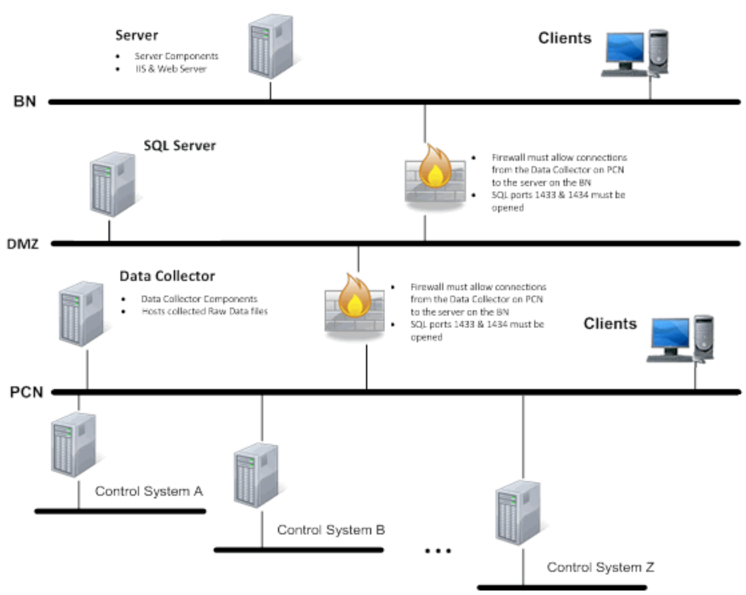
DMZ - Clients Available from Business Network or Process Control Network

This deployment option illustrates working with a DMZ, with a server on the Business Network (BN), and Integrity data collector on the Process Control Network (PCN). Clients are available from the Business Network or the Process Control Network.

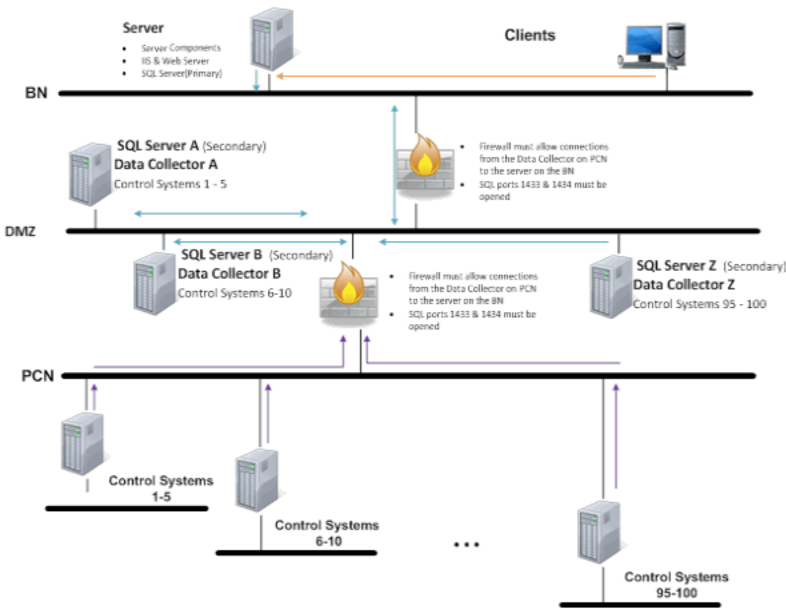


Separate Integrity Server & SQL Server with Additional Firewall Security

Web Clients are available on the Business Network (BN), with Server and SQL Server on the Process Control Network (PCN) with Web Clients access. This deployment is not recommended for Real-time Applications, due to access issues.



Shared Integrity Server & SQL Server with Distributed Databases



Integrity Server System Requirements

Integrity Server requirements depend on the overall deployment size. This section helps you determine whether your deployment is Size A, B, or C. The sections that follow provide detailed requirements for each computer type in each sized deployment.

Integrity Server requirements depend on the overall deployment size. This section helps you determine whether your deployment is Size A, B, or C. The sections that follow provide detailed requirements for each computer type in each sized deployment.

Size A - Small

Up to 10 simultaneous users

Up to 10 assets as listed in the Asset Equivalent List

Size B - Medium

Up to 10 simultaneous users

Up to 20 assets as listed in the Asset Equivalent List

Size C - Large

Up to 10 simultaneous users

Up to 50 assets as listed in the Asset Equivalent List

NOTE For deployments that exceed 50 assets as listed in the Asset Equivalent List, contact Technical Support for specific recommendations.

Asset Equivalent List

The following list summarizes how assets of different types impact the requirements for your deployment. For example, one DCS is equivalent to one asset, and 50 computers are equivalent to one asset when considering requirements.

Advanced Process Control (APC)

Every 10 of these assets are equivalent to 1 asset for hardware requirements.

Computers

Every 50 of these assets are equivalent to 1 asset for hardware requirements.

Distributed Control System (DCS)

Every 1 of these assets are equivalent to 1 asset for hardware requirements.

Historian

Every 1 of these assets are equivalent to 1 asset for hardware requirements.

Human Machine Interface (HMI)

5 of these assets are equivalent to 1 asset for hardware requirements.

Instrumentation Database

1 of these assets are equivalent to 1 asset for hardware requirements.

Programmable Logic Controller (PLC)

5 of these assets are equivalent to 1 asset for hardware requirements.

Safety Instrumented System (SIS)

2 of these assets are equivalent to 1 asset for hardware requirements.

Machinery Protection Condition Monitoring

5 of these assets are equivalent to 1 asset for hardware requirements.

Size A Small

Topics

Size A - Shared Integrity Server, Web Server, and SQL Server Computer

Computer/Processor

Server-grade computer with eight cores, 2 GHz processors or better.

RAM

Standard 64-bit: 24 GB.

Enterprise 64-bit: 24 GB.

NOTE Allocate at least 50% of the available RAM to SQL Server.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS drive at least 80 GB.

D: - Application drive at least 500 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

SQL Server Software

Microsoft SQL Server 2008 R2, 2012, 2014, 2016, 2017, or 2019 (Standard or Enterprise Edition).

Ensure that adequate User CAL, Device CAL, or Professional Licenses are available to cover the intended use of Integrity.

Enable FILESTREAM.

Install Full-Text and Semantic Extractions for Search, an optional component of the SQL Server Database Engine.

IIS Configuration

IIS (Internet Information Server) 7.0 or higher.

ASP.NET Framework 4.8 to be enabled.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Additional Software

Microsoft Visio 32-bit 2010 or later.

Microsoft Excel 2010 or later. Some asset models (e.g. Sensor Data Integrity or ABB Harmony) require data import from Excel files. For more information to determine whether an individual asset model has this requirement, see the Implementation Guide for that asset model. To facilitate this transfer from Microsoft Excel, you need Microsoft Access Database Engine on the data collector computers. The AccessDatabaseEngine.exe file is available in the Installation folder, or it is available for download from this site:
https://www.microsoft.com/en-us/download/details.aspx?id=13255
https://www.microsoft.com/en-us/download/details.aspx?id=13255.

Size A - Separate Web Server

Computer/Processor

Server-grade computer with four cores, 2 GHz processors or better.

RAM

Standard 64-bit: 16 GB.

Enterprise 64-bit: 16 GB.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS drive at least 80 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

IIS Configuration

IIS (Internet Information Server) 7.0 or higher.

ASP.NET Framework 4.8 to be enabled.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Additional Software

Microsoft Visio 32-bit 2010 or later.

Microsoft Excel 2010 or later. Some asset models (e.g. Sensor Data Integrity or ABB Harmony) require data import from Excel files. For more information to determine whether an individual asset model has this requirement, see the Implementation Guide for that asset model. To facilitate this transfer from Microsoft Excel, you need Microsoft Access Database Engine on the data collector computers. The AccessDatabaseEngine.exe file is available in the Installation folder, or it is available for download from this site:
https://www.microsoft.com/en-us/download/details.aspx?id=13255
https://www.microsoft.com/en-us/download/details.aspx?id=13255.

Size A - Separate SQL Server Computer

Computer/Processor

Server-grade computer with four cores, 2 GHz processors or better.

RAM

Standard 64-bit: 24 GB.

Enterprise 64-bit: 24 GB.

NOTE Allocate at least 50% of the available RAM to SQL Server.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS drive with at least 80 GB.

D: - Application and Database with at least 300 GB.

E: - Backup Drive at least 500 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

SQL Server Software

Microsoft SQL Server 2008 R2, 2012, 2014, 2016, 2017, or 2019 (Standard or Enterprise Edition).

Ensure that adequate User CAL, Device CAL, or Professional Licenses are available to cover the intended use of Integrity.

Enable FILESTREAM.

Install Full-Text and Semantic Extractions for Search, an optional component of the SQL Server Database Engine.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Size A - Separate Data Collector Server

Computer/Processor

Server-grade computer with four cores, 2 GHz processors or better

RAM

Standard 64-bit: 24 GB.

Enterprise 64-bit: 24 GB.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS Drive at least 80 GB.

D: - Application Drive to be at least 300 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Size B Medium

Topics

Size B - Shared Integrity Server, Web Server, and SQL Server Computer

Computer/Processor

Server-grade computer with 12 cores, 2 GHz processors or better.

RAM

Standard 64-bit: 48 GB.

Enterprise 64-bit: 48 GB.

NOTE Allocate at least 50% of the available RAM to SQL Server.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS drive at least 80 GB.

D: - Application drive at least 750 GB.

E: - Backup drive at least 500 GB

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

SQL Server Software

Microsoft SQL Server 2008 R2, 2012, 2014, 2016, 2017, or 2019 (Standard or Enterprise Edition).

Ensure that adequate User CAL, Device CAL, or Professional Licenses are available to cover the intended use of Integrity.

Enable FILESTREAM.

Install Full-Text and Semantic Extractions for Search, an optional component of the SQL Server Database Engine.

IIS Configuration

IIS (Internet Information Server) 7.0 or higher.

ASP.NET Framework 4.8 to be enabled.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Additional Software

Microsoft Visio 32-bit 2010 or later.

Microsoft Excel 2010 or later. Some asset models (e.g. Sensor Data Integrity or ABB Harmony) require data import from Excel files. For more information to determine whether an individual asset model has this requirement, see the Implementation Guide for that asset model. To facilitate this transfer from Microsoft Excel, you need Microsoft Access Database Engine on the data collector computers. The AccessDatabaseEngine.exe file is available in the Installation folder, or it is available for download from this site:
https://www.microsoft.com/en-us/download/details.aspx?id=13255
https://www.microsoft.com/en-us/download/details.aspx?id=13255.

Size B - Separate Web Server

Computer/Processor

Server-grade computer with four cores, 2 GHz processors or better.

RAM

Standard 64-bit: 16 GB.

Enterprise 64-bit: 16 GB.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS drive at least 80 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

IIS Configuration

IIS (Internet Information Server) 7.0 or higher.

ASP.NET Framework 4.8 to be enabled.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Additional Software

Microsoft Visio 32-bit 2010 or later.

Microsoft Excel 2010 or later. Some asset models (e.g. Sensor Data Integrity or ABB Harmony) require data import from Excel files. For more information to determine whether an individual asset model has this requirement, see the Implementation Guide for that asset model. To facilitate this transfer from Microsoft Excel, you need Microsoft Access Database Engine on the data collector computers. The AccessDatabaseEngine.exe file is available in the Installation folder, or it is available for download from this site:
https://www.microsoft.com/en-us/download/details.aspx?id=13255
https://www.microsoft.com/en-us/download/details.aspx?id=13255.

Size B - Separate SQL Server Computer

Computer/Processor

Server-grade computer with 12 cores, 2 GHz processors or better.

RAM

Standard 64-bit: 32 GB.

Enterprise 64-bit: 32 GB.

NOTE Allocate at least 50% of the available RAM to SQL Server.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS drive with at least 80 GB.

D: - Application and Database with at least 500 GB.

E: - Backup Drive at least 500 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

SQL Server Software

Microsoft SQL Server 2008 R2, 2012, 2014, 2016, 2017, or 2019 (Standard or Enterprise Edition).

Ensure that adequate User CAL, Device CAL, or Professional Licenses are available to cover the intended use of Integrity.

Enable FILESTREAM.

Install Full-Text and Semantic Extractions for Search, an optional component of the SQL Server Database Engine.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Size B - Separate Data Collector Server

Computer/Processor

Server-grade computer with eight cores, 2 GHz processors or better

RAM

Standard 64-bit: 24 GB.

Enterprise 64-bit: 24 GB.

Hard Disk

Recommend 10,000 RPM drives or better.

C: - OS Drive at least 80 GB.

D: - Application Drive to be at least 500 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Size C Large

Having the Web Server, Data Collector, and SQL Server shared on one computer in a large deployment is not recommended. Allocate separate servers for each of these components.

Topics

Size C - Separate Web Server

Computer/Processor

Server-grade computer with eight cores, 2 GHz processors or better.

RAM

Standard 64-bit: 24 GB.

Enterprise 64-bit: 24 GB.

Hard Disk

Recommend 10,000 RPM drives.

C: - OS drive at least 80 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

IIS Configuration

IIS (Internet Information Server) 7.0 or higher.

ASP.NET Framework 4.8 to be enabled.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Additional Software

Microsoft Visio 32-bit 2010 or later.

Microsoft Excel 2010 or later. Some asset models (e.g. Sensor Data Integrity or ABB Harmony) require data import from Excel files. For more information to determine whether an individual asset model has this requirement, see the Implementation Guide for that asset model. To facilitate this transfer from Microsoft Excel, you need Microsoft Access Database Engine on the data collector computers. The AccessDatabaseEngine.exe file is available in the Installation folder, or it is available for download from this site:
https://www.microsoft.com/en-us/download/details.aspx?id=13255
https://www.microsoft.com/en-us/download/details.aspx?id=13255.

Size C - Separate SQL Server Computer

Computer/Processor

Server-grade computer with 24 cores, 2 GHz processors or better.

RAM

Standard 64-bit: 64 GB.

Enterprise 64-bit: 64 GB.

NOTE Allocate at least 50% of the available RAM to SQL Server.

Hard Disk

Recommend 15,000 RPM drives or better.

C: - OS drive with at least 80 GB.

D: - Application drive and Database with at least 750 GB.

E: - Backup drive at least 2 TB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

SQL Server Software

Microsoft SQL Server 2008 R2, 2012, 2014, 2016, 2017, or 2019 (Standard or Enterprise Edition).

Ensure that adequate User CAL, Device CAL, or Professional Licenses are available to cover the intended use of Integrity.

Enable FILESTREAM.

Install Full-Text and Semantic Extractions for Search, an optional component of the SQL Server Database Engine.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Size C - Separate Data Collector

Computer/Processor

Server-grade computer with 12 cores, 2 GHz processors or better.

RAM

Standard 64-bit: 32 GB.

Enterprise 64-bit: 32 GB.

Hard Disk

Recommend 10,000 RPM drives.

C: - OS drive at least 80 GB.

D: - Application drive to be at least 750 GB.

Additional hard drive space might be required depending on site backup requirements.

Implementation of RAID-1 for the operating system and RAID 5, 6, or 10 for the Database Storage, Application, and Backup drives is recommended, following customer's data management policies.

RAID Controller should be high performance and cache enabled.

Operating System

Microsoft Windows 2008 R2, 2012, 2016, or 2019 Server (ANSI character set) Standard, Enterprise, or Datacenter Edition (64 bit).

Microsoft Installer v 3.1.

Microsoft .NET Framework 4.5 or later.

Microsoft .NET Framework should be installed prior to the installation of ODBC.Net Data Driver.

ODBC.Net Data Driver with Microsoft Data Access Components (MDAC) 2.8 or higher.

WebDAV Publishing should NOT be installed.

Network Connectivity

100 / 1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

The Integrity Web Server uses TCP/IP port 1433 for connecting to SQL Server (this port is configurable). The SQL Server browser service uses port 1434 to allow users to select server from list.

The Integrity clients use TCP/IP port 80 for connecting to the Integrity Web Server.

Email

Email server access from the Integrity Server is required for only emailing reports and diagnostics.

Integrity sends email using SMTP on TCP/IP Port 25. Some email applications block emails from going out to Port 25. This feature needs to be turned off in virus checking software on the Integrity Server.

Integrity Virtualization Requirements

To maintain the performance of Integrity, the Integrity Application Server (Web Server) and Data Collector may each be virtualized with the additional requirements identified in this section. All initial sizing requirements should be determined from the specifications in the system requirements sections, and increased by the additional requirements in this section. For more information and further clarification about Integrity virtualization requirements, contact Technical Support.

Computer

Should minimally meet the standards for either:

- Hyper V (Microsoft SVVP validation program) at *http://www.windowsservercatalog.com/svvp.aspx?svvppage=svvpwizard.htm* *http://www.windowsservercatalog.com/svvp.aspx?svvppage=svvpwizard.htm*
- VMware vSphere 5.1 at *http://www.windowsservercatalog.com/item.aspx?idItem=18c9ca52-dc8d-b817-c833-b096b65c67de&bCatID=1521* *http://www.windowsservercatalog.com/item.aspx?idItem=18c9ca52-dc8d-b817-c833-b096b65c67de&bCatID=1521*

Processor

Follow the guidelines from Microsoft when building your computer. Specific hyper-threading guidelines and best practices can be found at:

http://blogs.technet.com/b/keithmayer/archive/2012/08/30/virtualizing-microsoft-sql-server-on-windows-server-2012-winserv-mssql-itpro-sqlpass.aspx *http://blogs.technet.com/b/keithmayer/archive/2012/08/30/virtualizing-microsoft-sql-server-on-windows-server-2012-winserv-mssql-itpro-sqlpass.aspx*.

RAM

Recommended sizes from checklists, plus at least 25%.

Hard Disk

Hard disks should be actual drives in the main server and not network drives (SAN or NAS).

Dedicated I/O for hard disks per VM platform.

Operating System

Microsoft Server Virtualization Validation Program (SVVP) for the installed virtualized platform (Server 2008 or higher).

Network Connectivity

Dedicated Network Interface Card for the Virtualized Server.

Resources

Any components within a Virtual Environment should have the specified resources available at all times.

Integrity Client Requirements

To maintain the performance of Integrity, the following components are required for each client computer accessing Integrity.

Computer/Processor

Dual-core or one quad-core, 2 GHz processors or better.

RAM

4 GB.

Operating System

Microsoft Windows 7 or later.

Network Connectivity

100/1000 MBPS or better Ethernet network adapter and TCP/IP protocol are required.

Additional Software

Google Chrome, Chromium-based Microsoft Edge, or Internet Explorer 11.

NOTES

- Compatibility View should be turned off.
- JavaScript, also referred to as active scripting and active content, must be allowed.
- Internet Explorer Enhanced Security Configuration may need to be disabled so JavaScript can run.
- If Integrity windows do not display as expected, turn off popup blocking browser options.

Microsoft Visio Viewer.

Microsoft Excel 2010 or later. Some asset models (e.g. Sensor Data Integrity or ABB Symphony Plus) require data import from Excel files. For more information to determine if an individual asset model has this requirement, see the Implementation Guide for that asset model. To facilitate this transfer from Microsoft Excel, you need Microsoft Access Database Engine on the data collector computers. The AccessDatabaseEngine.exe file is available in the Installation folder, or it is available for download from the Microsoft site:
https://www.microsoft.com/en-us/download/details.aspx?id=13255
https://www.microsoft.com/en-us/download/details.aspx?id=13255.

Adobe Reader, if needed, for viewing PDF files requested from Integrity.

Support, Copyright, and Legal Information

Intergraph Corporation, Hexagon's Asset Lifecycle Intelligence Division
305 Intergraph Way
Madison, AL 35758

Documentation

Documentation shall mean, whether in electronic or printed form, User's Guides, Installation Guides, Reference Guides, Administrator's Guides, Customization Guides, Programmer's Guides, Configuration Guides and Help Guides delivered with a particular software product.

Other Documentation

Other Documentation shall mean, whether in electronic or printed form and delivered with software or on Smart Community, SharePoint, box.net, or the Hexagon documentation web site, any documentation related to work processes, workflows, and best practices that is provided by Hexagon as guidance for using a software product.

Terms of Use

a. Use of a software product and Documentation is subject to the Software License Agreement ("SLA") delivered with the software product unless the Licensee has a valid signed license for this software product with Intergraph Corporation, Hexagon's Asset Lifecycle Intelligence Division ("Hexagon"), a Hexagon Group Company. If the Licensee has a valid signed license for this software product with Hexagon, the valid signed license shall take precedence and govern the use of this software product and Documentation. Subject to the terms contained within the applicable license agreement, Hexagon gives Licensee permission to print a reasonable number of copies of the Documentation as defined in the applicable license agreement and delivered with the software product for Licensee's internal, non-commercial use. The Documentation may not be printed for resale or redistribution.

b. For use of Documentation or Other Documentation where end user does not receive a SLA or does not have a valid license agreement with Hexagon, Hexagon grants the Licensee a non-exclusive license to use the Documentation or Other Documentation for Licensee's internal non-commercial use. Hexagon gives Licensee permission to print a reasonable number of copies of Other Documentation for Licensee's internal, non-commercial use. The Other Documentation may not be printed for resale or redistribution. This license contained in this subsection b) may be terminated at any time and for any reason by Hexagon by giving written notice to Licensee.

Disclaimer of Warranties

Except for any express warranties as may be stated in the SLA or separate license or separate terms and conditions, Hexagon disclaims any and all express or implied warranties including, but not limited to the implied warranties of merchantability and fitness for a particular purpose and nothing stated in, or implied by, this document or its contents shall be considered or deemed a modification or amendment of such disclaimer. Hexagon believes the information in this publication is accurate as of its publication date.

The information and the software discussed in this document are subject to change without notice and are subject to applicable technical product descriptions. Hexagon is not responsible for any error that may appear in this document.

The software, Documentation and Other Documentation discussed in this document are furnished under a license and may be used or copied only in accordance with the terms of this license. THE USER OF THE SOFTWARE IS EXPECTED TO MAKE THE FINAL EVALUATION AS TO THE USEFULNESS OF THE SOFTWARE IN HIS OWN ENVIRONMENT.

Hexagon is not responsible for the accuracy of delivered data including, but not limited to, catalog, reference and symbol data. Users should verify for themselves that the data is accurate and suitable for their project work.

Limitation of Damages

IN NO EVENT WILL HEXAGON BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL INCIDENTAL, SPECIAL, OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF USE OR PRODUCTION, LOSS OF REVENUE OR PROFIT, LOSS OF DATA, OR CLAIMS OF THIRD PARTIES, EVEN IF HEXAGON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

UNDER NO CIRCUMSTANCES SHALL HEXAGON'S LIABILITY EXCEED THE AMOUNT THAT HEXAGON HAS BEEN PAID BY LICENSEE UNDER THIS AGREEMENT AT THE TIME THE CLAIM IS MADE. EXCEPT WHERE PROHIBITED BY APPLICABLE LAW, NO CLAIM, REGARDLESS OF FORM, ARISING OUT OF OR IN CONNECTION WITH THE SUBJECT MATTER OF THIS DOCUMENT MAY BE BROUGHT BY LICENSEE MORE THAN TWO (2) YEARS AFTER THE EVENT GIVING RISE TO THE CAUSE OF ACTION HAS OCCURRED.

IF UNDER THE LAW RULED APPLICABLE ANY PART OF THIS SECTION IS INVALID, THEN HEXAGON LIMITS ITS LIABILITY TO THE MAXIMUM EXTENT ALLOWED BY SAID LAW.

Export Controls

To the extent prohibited by United States or other applicable laws, Intergraph Corporation, Hexagon's Lifecycle Intelligence division ("Hexagon"), and a Hexagon Group Company's commercial-off-the-shelf software products, customized software, Technical Data, and/or third-party software, or any derivatives thereof, obtained from Hexagon, its subsidiaries, or distributors must not be exported or re-exported, directly or indirectly (including via remote access) under the following circumstances:

a. To Cuba, Iran, North Korea, Syria, or the Crimean, "Donetsk People's Republic", "Luhansk People's Republic," or Sevastopol regions of Ukraine, or any national of these countries or territories.
b. To any person or entity listed on any United States government denial list, including, but not limited to, the United States Department of Commerce Denied Persons, Entities, and Unverified Lists, the United States Department of Treasury Specially Designated Nationals List, and the United States Department of State Debarred List. Visit www.export.gov for more information or follow this link for the screening tool: *https://legacy.export.gov/csl-search https://legacy.export.gov/csl-search*.
c. To any entity when Customer knows, or has reason to know, the end use of the software product, customized software, Technical Data and/or third-party software obtained from Hexagon, its subsidiaries, or distributors is related to the design, development, production, or use of missiles, chemical, biological, or nuclear weapons, or other un-safeguarded or sensitive nuclear uses.
d. To any entity when Customer knows, or has reason to know, that an illegal reshipment will take place.

Any questions regarding export/re-export of relevant Hexagon software product, customized software, Technical Data, and/or third-party software obtained from Hexagon, its subsidiaries, or distributors, should be addressed to Hexagon's Export Compliance Department, 305 Intergraph Way, Madison, Alabama 35758 USA or at exportcompliance@intergraph.com. Customer shall hold harmless and indemnify Hexagon and a Hexagon Group Company for any causes of action, claims, costs, expenses and/or damages resulting to Hexagon or a Hexagon Group Company from a breach by Customer.

Trademarks

Intergraph®, the Intergraph logo®, Intergraph Smart®, SmartPlant®, SmartMarine, SmartSketch®, SmartPlant Cloud®, PDS®, FrameWorks®, I-Route, I-Export, ISOGEN®, SPOOLGEN, SupportManager®, SupportModeler®, SAPPHIRE®, TANK, PV Elite®, CADWorx®, CADWorx DraftPro®, GTSTRUDL®, CAESAR II® , and HxGN SDx® are trademarks or