Metasys Server Installation and Upgrade Instructions

MS-ADS05U-0, MS-ADX10U-0, MS-ADX10SQL-0, MS-ADX25U-0, MS-ADX25SQL-0, MS-ADX50U-0, MS-ADX50SQL-0, MS-ADX50SQL2-0, MS-ADX100U-0, MS-ADX100SQL2-0

Building Technologies & Solutions

www.johnsoncontrols.com

2021-07-02

LIT-12012162

Release 11.0

Contents

Welcome

Welcome to the Metasys Server Installation and Upgrade Instructions. The document guides you through the steps you need to follow to install or upgrade the Metasys Server software. In this document, the Metasys Server is also referred to as the Application and Data Server (ADS) or the Extended Application and Data Server (ADX).

Summary of Changes

The following information is new or revised:

- Updated the version numbers in Prerequisite Software Checklist for Installation and Upgrade for the Metasys products installed.
- Added support for Windows Server 2019 and removed support for Windows Server 2012 and Windows 7 as Metasys Server operating systems. Also, updated the service pack (SP) numbers and updates for supported products in Prerequisite Software Checklist for Installation and Upgrade and Recommended OS and SQL Server Combinations.
- Added support for SQL Server 2019 and removed support for SQL Server 2012. Also added required cumulative updates (CUs) to all affected SQL Server versions. See Prerequisite Software Checklist for Installation and Upgrade and Recommended OS and SQL Server Combinations. Refer to the *SQL Server Installation and Upgrade Instructions (LIT-12012240)* document for installing and upgrading your SQL Server software.
- Updated version number for Metasys Server software from Release 10.1 to 11.0 throughout document.
- Updated version number for SCT software from Release 13.2 to 14.0 throughout document.
- Updated supported Microsoft .NET Framework in Getting Started from 4.6.1 to 4.7.2.
- Updated In-Place Upgrade Considerations and Out-of-Place Upgrade Considerations with new information, including details about Basic Access and RADIUS user accounts.
- Added footnote to Prerequisite Software Checklist for Installation and Upgrade to indicate the Metasys Advanced Reporting System and Energy Essentials are compatible with SQL Server 2017, SQL Server 2016, and SQL Server 2014 software at Release 11.0, but are **not** compatible with SQL Server 2019.
- Added the installation requirement of the Metasys Server data file (.data) to Installing Metasys Server: Default Method and Installing Metasys Server: Custom Method.
- Added sections called Enabling and installing FIPS component and Uninstalling and unlicensing FIPS component.
- Removed the step for enabling the Windows component that Metasys UI requires called **Application Initialization** under Internet Information Services. The installer now enables this component for you.
- Described the option to install third-party applications required by the Metasys Server to a specific location in Installing Metasys Server: Custom Method.
- Added new section for customers who are using the Metasys Application Programming Interface (API): Customizing Windows IIS for Metasys API.
- Added new section Configuring Virtual Machine for Metasys Server.
- Updated installation sections to remind users to verify that all required software components are enabled.

- Added information about `Device archive failed (543)` error in the General Troubleshooting section.
- Renamed 'Database computer name' to 'application/web server name' in Database Server.
- Corrected all references of Windows Server 2016 to specify Version 10.0.14393.

Getting Started

The Metasys Server setup is a comprehensive utility that installs the Metasys Server, third-party components required by the Metasys Server software, and many of the Microsoft® Windows® components required by the Metasys system. The following tables list the components installed by the Metasys Server installer, unless already present. For the software listed under the **Components and Products NOT Installed** column, use the respective installation programs to add those components and applications.

Table 1: Components Installed and Not Installed by the Metasys Server

Windows® Components Installed	Metasys Products Installed	Components and Products NOT Installed
• Microsoft Internet Information Services (IIS) • Microsoft .NET Framework 4.7.2 • Microsoft Visual C++ Runtime Libraries • Microsoft Message Queuing (MSMQ) • Microsoft SQL Server® 2017 Express CU17 64-bit (ADS only) • Microsoft .NET Framework 3.5.1	• Application and Data Server (ADS) or Extended Application and Data Server (ADX) at Release 11.0 • Metasys UI Release 5.0 • Monitoring and Commanding API • Launcher 2.0 • Metasys Advanced Reporting System (ADX only) • Software Manager Release 3.0 • Metasys system databases	• SQL Server software (full version) • SQL Server Management Studio Express • System Configuration Tool (SCT) • Metasys for Validated Environments (MVE) • Energy Essentials • Metasys Export Utility • Metasys Database Manager

ⓘ **Note:** The Metasys Server setup attempts to install Microsoft .NET Framework 3.5.1 component. If the computer on which you are installing the Metasys Server software does not have access to Windows Updates, the installation of this component fails. In this case, install .NET Framework 3.5.1 manually.

The following table lists the third-party components installed with the Metasys Server Setup at Release 11.0.

Table 2: Third-Party Components Installed with the Metasys Server Setup

Third-Party Component	Brief Description
Erlang OTP 20 (9.0)	A required component for RabbitMQ functionality.
RabbitMQ Server 3.7.3	RabbitMQ is a service bus used to send notification messages to other services and is used for inter-process communication (messages) on the server.
Set Rate Limits	IIS module that applies rate limiting to Metasys API calls. This module and settings do not apply to SMP or MUI.

Licensing

The Metasys Server requires a software license for its base product. An application called Software Manager, installed with Metasys Server software, manages Metasys software licenses on a machine. We recommend that you license Metasys Server software immediately after installation. Also installed with the Metasys Server is the Monitoring and Commanding API, which is an optional feature that you need to purchase and license separately. Metasys UI, however, does not require a separate license. For information about activating licenses, refer to the *Starting a license activation* section in the *Software Manager Help (LIT-12012389)*.

Prerequisite Software Checklist for Installation and Upgrade

Before you begin with the Metasys Server installation or upgrade, review Table 3 to verify that you have the required software. The table also indicates where you can obtain each software component.

ⓘ **Note:** If you purchased Metasys Server software that includes SQL Server software (for example, MS-ADX25SQL-0), the SQL Server package is provided in a compressed file with a .rar file extension. This type of file is similar to a .zip file. Simply use a file extraction tool such as WinZip™ or 7-Zip File Manager to extract the .rar file to the server's hard drive.

ⓘ **Note:** Do not install Metasys on a Domain Controller. A Domain Controller provides the Active Directory service to network users and computers; stores directory data; and manages user and domain interactions including the login process, authentication, and directory searches.

Table 3: Prerequisite Software Checklist

	Software Component	Product	Where to Obtain
	Operating System (select one)[1]		
□	Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.[2]	ADS/SCT	Microsoft Corporation
□	Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)[2]		
□	Windows® Server® 2019 (version 1803 or later) (64-bit)	ADX/SCT	
□	Windows® Server® 2016 with Update (KB4512495) (64-bit)		
	Operating System (OS) Components (installed by Metasys Server)		
□	Internet Information Services (IIS) (included with OS)	ADS/ADX/ SCT	OS media
□	Microsoft Message Queuing (MSMQ)		
	Miscellaneous (select all)		
□	Microsoft .NET Framework 3.5 SP1 or 3.5.1	ADS/ADX/ SCT	OS Media
□	Microsoft .NET Framework 4.7.2 (installed by Metasys Server)		
□	Microsoft Silverlight® 5.0 or higher[3]		http://www.microsoft.com/silverlight
	Database (select one)		
□	SQL Server® 2019 Express (64-bit)	ADS/SCT	License Portal Microsoft Download Center
□	SQL Server® 2017 Express with CU17 (64-bit)		
□	SQL Server® 2016 Express with SP2 CU10 (64-bit)		
□	SQL Server® 2014 Express with SP3 CU4 (64-bit)		

Table 3: Prerequisite Software Checklist

	Software Component	Product	Where to Obtain
	SQL Server® 2019 (64-bit)[4] (Standard or Enterprise Edition)	ADX/SCT	Microsoft Corporation
❑	SQL Server® 2017 with CU17 (64-bit)[4] (Standard or Enterprise Edition)		
❑	SQL Server® 2016 with SP2 CU10 (64-bit)[4] (Standard or Enterprise Edition)		
❑	SQL Server® 2014 with SP3 CU4 (64-bit)[4] (Standard or Enterprise Edition)		
	Database Tools		
❑	SQL Installer Tool	ADS/SCT	License Portal
❑	Microsoft SQL Server Management Studio Express (ADS only)		License Portal or Microsoft Download Center
	Reporting Services		
❑	Microsoft Report Viewer 2012 Redistributable Package[5]	ADX	License Portal or Microsoft Corporation

[1] We highly recommend that the computer you want to use for Metasys software had its operating system installed on a cleanly formatted hard disk. If you use a computer that was upgraded from a previous version of Windows, files and registry settings left behind after the upgrade may adversely affect the installation of Metasys system software.

[2] Metasys system software does not support the touchscreen interface that is featured in the Windows 10 and Windows 8.1 operating systems.

[3] Required for viewing Graphics+ files on Site Management Portal software clients.

[4] At Release 11.0, Metasys Advanced Reporting System and Energy Essentials are compatible with SQL Server 2017, SQL Server 2016, and SQL Server 2014 software, but are **not** compatible with SQL Server 2019.

[5] Required for reports generated by the Metasys Advanced Reporting System or Metasys Energy Essentials. Use Report Viewer 2012 Redistribution Package for SQL Server 2017, SQL Server 2016, and SQL Server 2014 software.

Recommended OS and SQL Server Combinations

The following table lists by operating system the SQL Server software editions that have been fully qualified by Johnson Controls for the current release of Metasys Server. You can select other combinations, but we recommend that you select from the following pairings.

Table 4: Recommended Operating System and SQL Server Combinations

Operating System		Database Software							
		Desktop Computer Platform				Server Computer Platform			
		SQL Server ® 2019 Express (64-bit)	SQL Server® 2017 Express with CU17 (64-bit)	SQL Server® 2016 Express with SP2 CU10 (64-bit)	SQL Server ® 2014 Express with SP3 CU4 (64-bit)	SQL Server ® 2019 (64-bit)	SQL Server ® 2017 with CU17 (64-bit)	SQL Server ® 2016 with SP2 CU10 (64-bit)	SQL Server ® 2014 with SP3 CU4 (64-bit)
Desktop	Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	x	x	x	x				
	Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)		x	x	x				

Table 4: Recommended Operating System and SQL Server Combinations

Operating System		Database Software							
		Desktop Computer Platform				Server Computer Platform			
		SQL Server® 2019 Express (64-bit)	SQL Server® 2017 Express with CU17 (64-bit)	SQL Server® 2016 Express with SP2 CU10 (64-bit)	SQL Server® 2014 Express with SP3 CU4 (64-bit)	SQL Server® 2019 (64-bit)	SQL Server® 2017 with CU17 (64-bit)	SQL Server® 2016 with SP2 CU10 (64-bit)	SQL Server® 2014 with SP3 CU4 (64-bit)
Server	Windows® Server® 2019 (version 1803 or later) (64-bit)					x	x	x	x
	Windows® Server® 2016 with Update (KB4512495) (64-bit)					x	x	x	x

Pre-Work checklist for new installations and upgrades

Before you begin the process of installing or upgrading the Metasys Server at a customer site, follow the steps in the checklist below.

Table 5: Pre-work Checklist

Step	Action	Details
❏	Review related documentation	Download and review all the Flash Sheets, FYIs, and Quick Patches from the portal that relate to Metasys software installation and upgrades. Links to all these resources are available on the Field Support Center Find Answers page. Download and review all the relevant product literature from the Knowledge Exchange website. Knowledge Exchange has the most up-to-date versions of product literature.
❏	Verify that all available Windows updates have been applied to the Windows operating system on the target computer. Also make sure the versions of the OS and SQL Server software (if previously installed) are supported.	See Prerequisite Software Checklist for Installation and Upgrade. During the Metasys Server installation or upgrade process, a message may appear that prompts you to check that the version of SQL Server software is up to date.
❏	Understand steps for installing Metasys software on a virtual machine (VM)	If you are installing a virtual ADS/ADX server, ensure the virtual server is running in static memory mode, not dynamic. Otherwise, operational issues with SQL Server may occur. Also, if upgrading from hardware server to virtual, configure the ADS/ADX VM with the same amount of memory as the hardware ADS/ADX server, or with 8 GB of memory as a minimum.
❏	Verify Metasys Server computer has a minimum of 8 GB RAM	The Metasys installer requires at least 8 GB of memory or the install fails. The same holds true for installing on a virtual machine.
❏	Uninstall or upgrade existing release of SCT	If your computer has SCT 11.1 or earlier, plan to uninstall SCT before installing SCT Release 14.0. If your computer has SCT Release 12.0 or 13.x, you can upgrade to SCT Release 14.0 without removing the older version of SCT. During this upgrade, the newest version of the NAE Update Tool is also installed.
❏	Upgrade existing release of CCT	If your computer has CCT 13.1 or earlier, and you plan to use the NxE Passthru option in CCT with Metasys Release 11.0, you must upgrade to CCT Release 14.0.

Table 5: Pre-work Checklist

Step	Action	Details
❑	Uninstall or upgrade existing NAE Update Tool	If your computer has SCT 11.0 or earlier, plan to uninstall any older version of the NAE Update Tool if still present on the computer. If your computer has SCT 12.0 or later, you do not need to uninstall the NAE Update Tool, because upgrading SCT also upgrades the latest version of the NAE Update Tool. The stand-alone setup for the NAE Update Tool has been discontinued. If the job site does not allow your laptop on their network, install the SCT and the NAE Update Tool on the ADS/ADX server. When you are creating a full target list of network engines in the NAE Update Tool, save the Target file to your laptop with a descriptive name. If you need help with the NAE Update Tool, review the *Overview* section for the *NAE Update Tool Help (LIT-12011524)*.
❑	Bring along all necessary software updates and service packs	If your customer site does not have access to the Internet, download any Microsoft or other software patches and service packs onto a DVD or flash drive **before** you go to the site. Any newly installed Microsoft software must be registered, through the Internet or email/fax, which takes time.
❑	Check Network Engine Versions	Check the versions and memory usage of the NAE/NIEs installed at the site. The NxE55xx-0 and NAE45xx-0 models **cannot be upgraded** to Release 8.0 or later because they have insufficient memory and performance. Also, NIE55 models **cannot be upgraded** to Release 10.0 or later because they are no longer supported. To help you locate older NxEs, use the Metasys Supervisory Scan tool. You have two choices for these engines: replace the NxE or keep the engine at its current release. The NxE55xx-0, NAE45xx-0, and NIE55 models may coexist with servers running the latest Metasys version. In addition, the NCE25, NAE35, and NAE45 models cannot be upgraded beyond Release 9.0.8, and the LON models of these engines cannot be upgraded beyond Release 9.0. Lastly, all modem and pager functions on network engines are no longer functional with the Release 9.0.7 or later upgrade.
❑	Check for NxE55xx-1 Engines	If the site has NxE55xx-1 models, review Flash Sheet 2013F21. This Flash Sheet has you check for bad memory by using the Field Bus Fault Detection and Diagnostic (FDD) Tool.

Table 5: Pre-work Checklist

Step	Action	Details
❑	Create a network engine report	Use the Metasys Supervisory Tool or Tailored Summaries to print out a summary of the network engines operating at the site. The network engine information that is most helpful includes: • the current online condition and IP address • the current software release • the current memory usage. If a network engine is currently running at >95% of Flash memory usage, you may have issues with the upgrades, since features requiring more memory may be added.
❑	Decide which network engines to update	It is not necessary to update all the network engines on the site immediately. You can keep some network engines at their existing release. You only need to upgrade the Site Director to the new release. You can delay the upgrade of critical engines to off-hours or extend the upgrade schedule across a number of site visits. ➧ **Important:** After you install or upgrade the Metasys Server to Release 11.0, the Site object attribute called **Advanced Security Enabled** is set to True, so that any network engine not at Release 10.0 or later no longer communicates to the server. You have two options: (1) update all network engines to Release 10.0 or later or (2) do not update the network engines to Release 10.0 or later and change the **Advanced Security Enabled** on the Site object to False.
❑	Arrange for updating network engines over individual subnets	When you update a network engine from Release 9.0 or earlier to Release 9.0.7 or later, you must use SCT Pro 14.0 or the NAE Update Tool with the PXE only option. You **cannot** use SCT 13.2 to update the network engine. Also, the update can only occur on the same subnetwork, so special arrangements might be required to access remote engines.
❑	Plan for and be aware of new field controller limitations for new SNE and SNC network engines	The SNE and SNC network engines have fixed limits for the number of field controller that they support, which are listed in the *SNE/SNC Product Bulletin (LIT-12013296)*. If you plan to replace an NAE with an SNE, or an NCE with an SNC, be aware of these newly enforced limitations. If you have any NAE/NCE that has a higher device count than the limits, plan to redistribute field controllers to different SNE/SNC engines.
❑	Verify that the network card on the computer or VM you selected for the Metasys Server has a valid IP address and an active network connection	Before you begin the installation or upgrade, make sure that the network card on the computer or VM for the Metasys Server is enabled and connected to the building network with a valid IP address. For a successful installation or upgrade, the Metasys Installer must be able to read the MAC address of the network card.

Table 5: Pre-work Checklist

Step	Action	Details
❑	Verify Port 443 is open and handles traffic in the same manner as Port 80	Check with IT and verify how the networking equipment handles Port 80 traffic. The same type of treatment is needed for Port 443. Refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.
❑	Review Graphics	Review and print to a PDF file the existing conditions of the graphics for all major equipment, such as chilled water system, cooling towers, air handlers, exhaust fans, boilers, and any others.
❑	Generate reports	Review and print to a PDF file the Override, Offline, Disabled, and Alarm Reports for the entire network. These reports are available from the Query menu in the Site Management Portal (SMP) UI. Also, review and print NAE Diagnostics, NAE Unbound References, and Field Bus diagnostics for the network. This data is helpful when you return the system back to a pre-upgrade state.

Metasys Server Installation

This section includes the steps for **installing** Metasys Server software. Before you begin the installation process, make sure you review Pre-Work checklist for new installations and upgrades.

If you instead need to upgrade existing Metasys Server software, see Metasys Server In-Place Upgrade or Metasys Server Out-of-Place Upgrade.

Which type of Metasys Server are you installing?	
Unified ADS	Select to install the Metasys Server on a **desktop** operating system.
Unified ADS with SCT	Select to install the Metasys Server and SCT on a **desktop** operating system.
Unified ADX	Select to install the Metasys Server on a **server-class** operating system.
Unified ADX with SCT	Select to install the Metasys Server and SCT on a **server-class** operating system.
Split ADX with SCT	Select to install a split Metasys Server where database component is installed on one server-class system, the web/application component is installed on another server-class operating system, and SCT is installed on a desktop or server-class operating system.

Installing Unified Metasys Server on Desktop OS

Table 6: Supported Platforms Unified Metasys Server on Desktop OS

Supported Operating System	Supported Database Options
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	SQL Server® 2019 Express (64-bit) SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)

Use the steps in the following table for installing and configuring the Metasys Server software on a computer with a desktop operating system.

Table 7: Installing Unified Metasys Server on Desktop OS

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software has one of the following supported Windows desktop operating systems: • Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. • Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows 10: Version 1903 10.18362 • Windows 8.1 with Update 1: Version 6.3.9600 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.

Table 7: Installing Unified Metasys Server on Desktop OS

Step	Action	Reference or Additional Steps
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
8.	Select the appropriate action: • If you want to allow the Metasys Server setup program to automatically choose where historical databases are created, skip to the next step. • If you want to specify a custom location for the Metasys historical databases (for example, E: drive), follow the step on the right.	See Specifying Custom Locations for Metasys Server Application and Databases. This section explains how to install SQL Server software and SQL Server Management Studio to the alternate disk drive (for example, E: drive). After completing the SQL Server installation steps, follow the next step below.
9.	If you want the Metasys Server to use trusted certificates instead of self-signed certificates (the default), configure the certificates on the Metasys Server before installing the software. Otherwise, go to the next step.	See Appendix: Certificate management and security.
10.	Install the Metasys Server software, which also installs a supported version of SQL Server software.	See Installing Metasys Server: Default Method. However, if you want to install to an alternate disk drive, see Installing Metasys Server: Custom Method.
11.	License the Metasys ADS software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
12.	Start Launcher and add a profile for the Site Management Portal (SMP).	Refer to *Launcher Tool Help (LIT-12011742)*.

Table 7: Installing Unified Metasys Server on Desktop OS

Step	Action	Reference or Additional Steps
13.	Start Metasys SMP from the Launcher and verify proper operation.	See Launching the User Interfaces.
14.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
15.	Install the Metasys Database Manager.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
16.	If prompted, restart the computer.	Use the standard procedure to restart the operating system.
17.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.

Installing Unified Metasys Server on Server OS

Table 8: Supported Platforms Unified Metasys Server on Server OS

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for installing and configuring the Metasys Server software on a computer with a server operating system.

Table 9: Installing Unified Metasys Server on Server OS

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 9: Installing Unified Metasys Server on Server OS

Step	Action	Reference or Additional Steps
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`. On server-class OSs, use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
8.	Install a supported version of SQL Server Standard or Enterprise software to the C: drive (primary partition), including the recommended cumulative update, if any. Select the Database Engine Services and Management Tools components. If you are installing SQL Server 2016 or SQL Server 2014, also select Reporting Services. If you are installing SQL Server 2019 or SQL Server 2017, use the standalone Reporting Services installer. ⓘ **Note:** If you want to install SQL Server software to an alternative disk drive (for example, E: drive), you need to follow some special steps. For details, see Specifying Custom Locations for Metasys Server Application and Databases.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*. For the Reporting Services installer, download the version that you need: SQL Server 2019 Reporting Services or SQL Server 2017 Reporting Services.

Table 9: Installing Unified Metasys Server on Server OS

Step	Action	Reference or Additional Steps
9.	If you intend to use the Metasys Advanced Reporting System or Energy Essentials, verify that Reporting Services is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
10.	Install support files if you plan to offer the Site Management Portal in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
11.	If you want the Metasys Server to use trusted certificates instead of self-signed certificates (the default), configure the certificates on the Metasys Server before installing the software. Otherwise, go to the next step.	See Appendix: Certificate management and security.
12.	Install the Metasys Server software.	See Installing Metasys Server: Default Method. However, if you want to install to an alternate disk drive or will be installing an ADX with Advanced Reporting, see Installing Metasys Server: Custom Method.
13.	License the Metasys ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
14.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
15.	Start Launcher and add a profile for the Site Management Portal (SMP).	Refer to *Launcher Tool Help (LIT-12011742)*.
16.	Start Metasys SMP from the Launcher and verify proper operation.	See Launching the User Interfaces.
17.	Install the Metasys Database Manager.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
18.	If prompted, restart the computer.	Use the standard procedure to restart the operating system.
19.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.

Installing Unified Metasys Server and SCT on Desktop OS

Table 10: Supported Platforms Unified Metasys Server on Desktop OS with SCT

Supported Operating System	Supported Database Options
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	SQL Server® 2019 Express (64-bit) SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)

Use the steps in the following table for installing and configuring the Metasys Server and SCT software on a computer with a desktop operating system.

Table 11: Installing Unified Metasys Server and SCT on Desktop Computer

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software has one of the following supported Windows desktop operating systems: • Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. • Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows 10: Version 1903 10.18362 • Windows 8.1 with Update 1: Version 6.3.9600 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.

Table 11: Installing Unified Metasys Server and SCT on Desktop Computer

Step	Action	Reference or Additional Steps
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
8.	Follow the appropriate step: • If you want to allow the setup program to automatically choose where historical databases are created, skip to the next step. • If you want to specify a custom location for the Metasys historical databases (for example, E: drive), follow the step on the right.	See Specifying Custom Locations for Metasys Server Application and Databases. This section explains how to install SQL Server software and SQL Server Management Studio to the alternate disk drive (for example, E: drive). After completing the SQL Server installation steps, follow the next step below.
9.	If you want the Metasys Server to use trusted certificates instead of self-signed certificates (the default), configure the certificates on the Metasys Server before installing the software. Otherwise, go to the next step.	See Appendix: Certificate management and security.
10.	Install and license SCT 14.0 software.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067).*
11.	Start Launcher and add a profile for Metasys SCT.	Refer to *Launcher Tool Help (LIT-12011742).*
12.	Start Metasys SCT from Launcher to verify operation.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067).*

Table 11: Installing Unified Metasys Server and SCT on Desktop Computer

Step	Action	Reference or Additional Steps
13.	Install the Metasys Server software, which also installs a supported version of SQL Server software.	See Installing Metasys Server: Default Method. However, if you want to install to an alternate disk drive, see Installing Metasys Server: Custom Method.
14.	License the Metasys ADS software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
15.	Start Launcher and add a profile for the Site Management Portal (SMP).	Refer to *Launcher Tool Help (LIT-12011742)*.
16.	Start Metasys SMP from the Launcher and verify proper operation.	See Launching the User Interfaces.
17.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
18.	Install the Metasys Database Manager.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
19.	If prompted, restart the computer.	Use the standard procedure to restart the operating system.

Installing Unified Metasys Server and SCT on Server OS

Table 12: Supported Platforms Unified Metasys Server with SCT Server OS

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for installing and configuring the Metasys Server and SCT software on a computer with a server operating system.

Table 13: Installing Unified Metasys Server and SCT on Server OS

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 13: Installing Unified Metasys Server and SCT on Server OS

Step	Action	Reference or Additional Steps
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`. On server-class OSs, use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
8.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
9.	Install a supported version of SQL Server Standard or Enterprise software to the C: drive (primary partition), including the recommended cumulative update, if any. Select the Database Engine Services and Management Tools components. If you are installing SQL Server 2016 or SQL Server 2014, also select Reporting Services. If you are installing SQL Server 2019 or SQL Server 2017, use the standalone Reporting Services installer. ⓘ **Note:** If you want to install SQL Server software to an alternative disk drive (for example, E: drive), you need to follow some special steps. For details, see Specifying Custom Locations for Metasys Server Application and Databases.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*. For the Reporting Services installer, download the version that you need: SQL Server 2019 Reporting Services or SQL Server 2017 Reporting Services.

Table 13: Installing Unified Metasys Server and SCT on Server OS

Step	Action	Reference or Additional Steps
10.	If you intend to use the Metasys Advanced Reporting System or Energy Essentials, verify that Reporting Services is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
11.	Install support files if you plan to offer the Site Management Portal in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
12.	If you want the Metasys Server to use trusted certificates instead of self-signed certificates (the default), configure the certificates on the Metasys Server before installing the software. Otherwise, go to the next step.	See Appendix: Certificate management and security.
13.	Install and license SCT 14.0 software.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
14.	Start Launcher and add a profile for Metasys SCT.	Refer to *Launcher Tool Help (LIT-12011742)*.
15.	Start Metasys SCT from Launcher. If you will be installing Metasys Advanced Reporting, create a new archive that you can later select in the Reporting tab of the Metasys Server setup window.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
16.	Install the Metasys Server software.	See Installing Metasys Server: Default Method. However, if you want to install to an alternate disk drive or will be installing an ADX with Advanced Reporting, see Installing Metasys Server: Custom Method.
17.	License the Metasys ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
18.	Install and license any other Metasys software (for example, Metasys Export Utility and Energy Essentials).	Refer to their respective installation documents.
19.	Start Launcher and add a profile for the Site Management Portal (SMP).	Refer to *Launcher Tool Help (LIT-12011742)*.
18.	Start Metasys SMP from the Launcher and verify proper operation.	See Launching the User Interfaces.
20.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
21.	Install the Metasys Database Manager.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
22.	If prompted, restart the computer.	Use the standard procedure to restart the operating system.

Installing a Split Metasys Server and SCT

Installing a split Metasys system with SCT involves three computers:

- SCT Computer
- Database Server
- Web/Application Server

ⓘ **Note:** Always set up the SCT computer first.

SCT Computer

Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)* for more information on supported platforms and for installing SCT.

Use the steps in the following table for installing SCT on a split Metasys system.

Table 14: Installing SCT Software on Split Metasys System

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for SCT software is running one of the following supported operating systems: • Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. • Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit) • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows 10: Version 1903 10.18362 • Windows 8.1 with Update 1: Version 6.3.9600 • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software. **For Windows 8.1 only:** start Windows Powershell and run the following command to verify that Update 1 (KB2919355) is installed: `get-hotfix -id KB2919355`. If the hotfix is not found, update the computer to Windows 8.1 with Update 1.
2.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
3.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
4.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 14: Installing SCT Software on Split Metasys System

Step	Action	Reference or Additional Steps
5.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`. On server-class OSs, use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
6.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
7.	Install a supported version of SQL Server software on a server class machine, including the recommended cumulative update, if any. The SCT setup installs SQL Server 2017 Express with CU17 on a non-server box if no SQL is present.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
8.	If you want the Metasys SCT to use trusted certificates instead of self-signed certificates (the default), configure the certificates on the Metasys SCT before installing the software. Otherwise, go to the next step.	See Appendix: Certificate management and security.
9.	Install and license SCT 14.0 software.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.

Table 14: Installing SCT Software on Split Metasys System

Step	Action	Reference or Additional Steps
10.	Start Launcher and add a profile for Metasys SCT.	Refer to *Launcher Tool Help (LIT-12011742)*.
11.	Start Metasys SCT from Launcher. If you will be installing Metasys Advanced Reporting, create a new archive that you can later select in the Reporting tab of the Metasys Server setup window.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
12.	Go to the next section to install the database server of the split ADX.	Go to Database Server.

Database Server

Table 15: Supported Platforms Split Metasys Server for Database Computer

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for installing the database component of the ADX on a split Metasys system.

Table 16: Installing Database Computer of Split Metasys System

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
3.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
4.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 16: Installing Database Computer of Split Metasys System

Step	Action	Reference or Additional Steps
5.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`. On server-class OSs, use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
6.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
7.	Install a supported version of SQL Server Standard or Enterprise software, including the recommended cumulative update, if any. Select the **Database Engine Services** and **Management Tools** components.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
8.	Install the Metasys Database Manager.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
9.	If prompted, restart the computer.	Use the standard procedure to restart the operating system.
10.	Go to the next section to install the web/ application server of the split ADX.	Go to Web/Application Server.

Web/Application Server

Table 17: Supported Platforms Split Metasys Server for Web/Application Computer

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for installing the web/application component of the ADX on a split Metasys system.

Table 18: Installing Web/Application Computer of Split Metasys System

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.

Table 18: Installing Web/Application Computer of Split Metasys System

Step	Action	Reference or Additional Steps
4.	Follow the appropriate step: • If you are installing the Metasys Server software on an English language computer, skip to the next step. • If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software feature installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. Click the **Microsoft .NET Framework 3.5** or **.NET Framework 3.5** feature. Check the **HTTP Activation** component. If you do not have Internet access, insert the operating system media, open a Command prompt with Run as Administrator, and execute this command (where <drive> is the disk drive with the media): `Dism /online /enable-feature /featurename:NetFx3 /All /Source:<drive>:\sources\sxs /LimitAccess`. On server-class OSs, use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.

Table 18: Installing Web/Application Computer of Split Metasys System

Step	Action	Reference or Additional Steps
8.	Install a supported version of SQL Server software, including the recommended cumulative update, if any. If you are using SQL Server 2016 or SQL Server 2014, select the **Reporting Services** and **Management Tools** components, but not the Database Engine Services component. If you are using SQL Server 2019 or SQL Server 2017, use the standalone Reporting Services installer.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*. For the Reporting Services installer, download the version that you need SQL Server 2017 Reporting Services.
9.	If you intend to use the Metasys Advanced Reporting System or Energy Essentials, configure Reporting Services.	Refer to the *Configuring SQL Server Reporting Services for the Metasys Advanced Reporting System* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
10.	Install support files if you plan to offer the Site Management Portal in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
11.	If you want the Metasys Server to use trusted certificates instead of self-signed certificates (the default), configure the certificates on the Metasys Server before installing the software. Otherwise, go to the next step.	See Appendix: Certificate management and security.
12.	Install the Metasys Server software, selecting the database server for the database component of the split ADX, the web/application server for the Metasys Reporting component of the split ADX, and the remote SCT and Data server systems for the Metasys Advanced Reporting feature.	See Installing Metasys Server: Custom Method.
13.	License the Metasys ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
14.	Install and license any other Metasys software (for example, Metasys Export Utility and Energy Essentials).	Refer to their respective installation documents.
15.	Start Launcher and add a profile for the Site Management Portal (SMP).	Refer to *Launcher Tool Help (LIT-12011742)*.
16.	Start Metasys SMP from the Launcher and verify proper operation.	See Launching the User Interfaces.

Table 18: Installing Web/Application Computer of Split Metasys System

Step	Action	Reference or Additional Steps
17.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
18.	If prompted, restart the computer.	Use the standard procedure to restart the operating system.
19.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.

Metasys Server In-Place Upgrade

This section includes the steps for performing an **in-place upgrade** of the ADS or ADX software to Metasys Server 11.0. An in-place upgrade is for upgrading an existing Metasys system on the same computer using the same version or upgraded version of SQL Server software. (This upgrade selection also applies if you need to update SQL Server software to a newer service pack.) Before upgrading to Metasys Server 11.0 software, make sure you review Pre-Work checklist for new installations and upgrades and Table 19.

Which type of Metasys Server are you upgrading?	
Unified ADS	Select to upgrade a Metasys Server on a **desktop** operating system.
Unified ADS with SCT	Select to upgrade a Metasys Server and SCT on a **desktop** operating system.
Unified ADX	Select to upgrade a Metasys Server on a **server-class** operating system.
Unified ADX with SCT	Select to upgrade a Metasys Server and SCT on a **server-class** operating system.
Split ADX with SCT	Select to upgrade a Metasys Server and SCT on a split configuration. With a split ADX, the database component is installed on one **server-class** system, the web/application component is installed on another **server-class** operating system, and SCT is installed on either a **server-class** or **desktop** operating system.

In-Place Upgrade Considerations

Before starting the in-place upgrade process, review the following table.

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Current condition of all Metasys system software	Before you start the upgrade, make sure that all currently loaded Metasys software applications are functioning properly. In particular, verify these applications: Metasys Database Manager, Metasys Export Utility, and Metasys UI.	Refer to the respective help systems and user guides.
Current operation of the Metasys Advanced Reporting system and Energy Essentials software	If the job site has an ADX that uses the Metasys Advanced Reporting System (ARS) and Energy Essentials, make sure that these applications are functioning properly. If ARS is installed but is not working or is corrupt, you may not be able to successfully perform an in-place upgrade. If this is the case, fully uninstall the ADX, then reinstall the ADX with Advanced Reporting at Release 10.1 before you upgrade.	To uninstall the ADX, see Uninstalling Metasys Server Software.
Current version of Windows operating system.	Before you start the upgrade, make sure that the current operating system is supported. If not, apply the required updates to match the versions listed here. ⓘ **Note: For Windows 8.1 only**, start Windows Powershell and run the following command to verify that Update 1 (KB2919355) is installed: get-hotfix -id KB2919355. If the hotfix is not found, update the computer to Windows 8.1 with Update 1.	To verify the Windows operating system, open a command prompt window and run the command **msinfo32**. Verify the version is at this level or higher: **Windows 10:** Version 1903 10.18362 **Windows 8.1:** Version 6.3.9600 **Windows Server 2019:** Version 10.0.118362 **Windows Server 2016**: Version 10.0.14393

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Current version of Microsoft® SQL Server® Software	If your Metasys system is currently using a version of SQL Server software that is no longer supported, you need to upgrade to a newer version. The Metasys Server installer halts if it detects the currently installed version, service pack, and cumulative update (CU) of SQL Server is not unsupported. For a list of supported SQL Server versions, SPs, and CUs, see Prerequisite Software Checklist for Installation and Upgrade.	See Verifying your computer has a supported version of SQL Server software installed. For more information on installing or upgrading SQL Server software, refer to the *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
Current version of ADS/ADX software	If the computer has ADS/ADX software at Release 7.x or earlier, you need to uninstall the existing ADS/ADX software. When prompted, select to **remove** license keys because you are upgrading to a new major software release. If the computer has ADS/ADX software at Release 8.x or later, you can choose the upgrade path instead of uninstalling first. You also need to uninstall ADS/ADX software if you are upgrading to a different software build at the **same** release level (for example, 11.0.0.3570 to 11.0.0.3847). After the uninstall, you can install the newer build.	See Uninstalling the Metasys Server Software Introduction.
Overall current condition of HVAC systems monitored by Metasys	Run and print out an Alarm summary and Override summary to document any existing system issues.	*Metasys Site Management Portal Help (LIT-1201793)*.
Windows Event Viewer	Check the Windows Event Viewer for any system, ADS, and MDM error messages.	Consult the Windows operating system documentation.

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Available hard disk space	Verify available disk space and clean up any miscellaneous and temporary files that can be removed to recover disk space.	Consult the Windows operating system documentation.
Security Database	If the current Metasys system is at **Release 5.2 or earlier**, log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. If the current Metasys system is at **Release 6.0 or later**, no separate security database backup is required because the security database is part of the archive database. Backing up the archive backs up security as well.	Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
Archive database	Using the existing release of SCT, upload the archive database, making sure you select the Include Security option. Then, create a database backup of the archive. Also create an export of the database with SCT. Backups are found in C:\ProgramData\Johnson Controls\MetasysIII\DatabaseFiles	*Upload*, *Backing Up an Archive Database*, and *Export Database* sections of the *Metasys SCT Help (LIT-12011964)*.

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
User accounts and passwords	Gather any applicable administrator user names and passwords that are required for installing or upgrading software. This includes the SQL System Administrator (sa) account and password. For customers who do not want to share these credentials, arrange for the SQL DBA to assist. Alternatively, the DBA can create a temporary SQL admin account with SA privileges just for the installation of the software, which you can delete later.	Consult the customer's IT administration.
User accounts with passwords that have not been recently modified or were created with an older release of Metasys that had different password requirements	To comply with the FIPS 140-2 standard, security changes to passwords were made at Metasys Release 11.0. At Release 8.1 and earlier, passwords were stored in a SHA1-hashed format, which is not FIPS compliant. Therefore, if you are upgrading your Metasys system from Release 8.1 or earlier, passwords of user accounts are reset with a default password that you specify during the archive upgrade process. To prevent user lock out for existing users, verify that the Never Expire property under Account Policy is not set. Additionally, set a new password for any user who has not changed their password in more than two years.	*Security Administrator System Technical Bulletin (LIT-1201528)*

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Basic access user accounts	Basic access users and the BasicSysAgent user account are no longer available at Release 11.0. The BasicSysAgent account is removed and all users with Basic access are converted to Standard access users when you upgrade the archive to SCT Release 14.0.	*Security Administrator System Technical Bulletin (LIT-1201528)*
RADIUS user accounts	RADIUS user accounts are no longer supported at Release 11.0. During the database archive upgrade process with SCT 14.0, each RADIUS user account in the archive is converted to a Metasys local user with an undefined password and a locked account. To activate the converted RADIUS account, a Metasys user with Administrator rights sets an initial password and unlocks the account.	*Security Administrator System Technical Bulletin (LIT-1201528)*
Preferences	System preferences do not persist during an upgrade to Release 11.0. Save your preference files to a safe location **before** the upgrade, and then move the files back to the appropriate location after the upgrade is complete. The preferences you need to save might include special alarm sound files and color selections, startup views, and links to external applications. Beginning with SCT 11.0, the upload and download processes include user preferences. However, SCT does not upload user preferences from a Site Director NAE.	*Configuring and Maintaining Preferences Appendix* of the *ADS/ADX Commissioning Guide (LIT-1201645)* or the *NAE Commissioning Guide (LIT-1201519)*.

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Object lists	Object lists stored in network engines do not persist during an upgrade to Release 11.0. Object lists are saved as files by the Global Search feature when you save search results. Save your object list files to a safe location **before** the upgrade, and then move the files back to the appropriate location after the upgrade is complete. Beginning with SCT 11.0, the upload and download processes include the object lists. However, SCT does not upload object lists from a Site Director NAE.	*Configuring and Maintaining Preferences Appendix* of the *ADS/ADX Commissioning Guide (LIT-1201645)* or the *NAE Commissioning Guide (LIT-1201519)*.
Customized config or properties files[1]	If you have customized files for your system, be sure to note those customizations before you upgrade. When you upgrade, these files are overwritten, and you lose your custom settings. After the upgrade, be sure to reapply your custom settings. ⓘ **Note:** When upgrading, do not replace the new file with a copy of the old file. Other settings in the file may have been changed to improve system performance or support new features. **Instead of replacing the new file with a copy of the old one, reapply the custom settings in the new file.**	Documentation for each specific product covers customization procedures, or you may be directed to update files by support personnel.

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Historical data	Install the Metasys Database Manager on the Metasys Server if it is not already present. Then, hours before you plan the system upgrade, use Metasys Database Manager to back up the historical databases, which include audit (JCIAuditTrails), alarm (JCIEvents), trend (JCIHistorianDB), annotation (JCIItemAnnotation), Metasys UI trends (JCIReportingDB), and reporting system (MetasysReporting). We recommend that you select the reindexing option, even though it significantly increases the length of time for this process. ⓘ **Note:** If the existing system is allowed to run post database backup, there will be gaps in the historical data from when the backup is completed until when the databases are migrated to the new server and it is brought online.	For installation steps, refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*. Then, refer to the *Backing Up a Database* section of the *Metasys Database Manager Help (LIT-12011202)*.
Metasys UI Spaces Authorization (SpacesAuthorization)	If upgrading from Metasys Release 8.0 or 8.1, use SQL Server Management Studio to back up the SpacesAuthorization database because the backup operation for that database is not available with Metasys Database Manager Release 8.0 or 8.1.	Consult the SQL Server Management Studio documentation.

Table 19: In-Place upgrade considerations

Data or Item	Details	Reference or Action
Coexisting versions of Metasys Server and SCT software.	The Metasys Server 11.0 may coexist on the same computer as SCT 14.0.	Refer to *SCT Installation and Upgrade Instructions (LIT-12012067)*.
BACnet Encoding Type	The archive upgrade process changes the BACnet Encoding Type attribute under the Site object. When a site is upgraded to Release 11.0 with SCT 14.0, the BACnet Encoding Type for the Site object is automatically changed to ISO 10646 UTF-8 during the archive upgrade process. If you require UCS-2 as the BACnet Encoding Type, make sure you set this attribute back to **UCS-2** after the archive upgrade is complete.	Refer to Site Object - Attributes section of *Metasys SMP Help (LIT--1201793)*.
Device pairing	At Metasys Release 10.0, a more secure authentication process was implemented between updated NxEs and the Site Director that involves device pairing. This capability is controlled by a new attribute in the Site object called **Advanced Security Enabled**. If you upgrade to Release 11.0 from an older release, Advanced Security Enabled is defaulted to **True** and NxEs become unpaired with their Site Directors.	Before upgrading to Release 11.0 (or before upgrading to a new build of Release 11.0), follow these steps: 1. Pair all network engines to the Metasys Server. 2. Using SCT, upload the Metasys Server with security to save the pairing information to the archive. 3. Perform the Metasys Server upgrade, but do not update the engines. 4. Using SCT, perform a Security Copy to the newly upgraded Metasys Server. 5. Verify all engines are now paired.

[1] The .config files contain custom Metasys network settings for features including serial printing Destination Delivery Agent (DDA) settings for an NAE, the Metasys Advanced Reporting System ADX, and the Action Queue in SCT. Examples of .config files you may have customized include web.config and ActionQueue.exe.config. Properties files also contain information related to name resolution and other system settings.

Upgrading Unified Metasys Server on Desktop OS

Table 20: Supported Platforms Unified Metasys Server on Desktop OS

Supported Operating System	Supported Database Options
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	SQL Server® 2019 Express (64-bit) SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)

Use the steps in the following table for upgrading the Metasys Server software on a computer with a desktop operating system.

Table 21: Upgrading Unified Metasys Server on Desktop Computer (In-Place)

Step	Action	Reference or Additional Steps
1.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
2.	Check if the computer has a SHA256 self-signed certificate bound to Default Web Site in IIS. If the ADS/ADX computer has a purchased certificate from a certificate authority (CA), determine if this is a SHA256 (Secure Hash Algorithm) certificate. If so, follow the steps on the right. If not, skip to the next step. Also, for more details, refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start IIS Manager. Expand the server, then expand Sites. 3. Click **Default Web Site**. Click **Bindings** in the right pane. The Site Bindings window appears. 4. Look for a Site Binding called **Type: https, Port: 443**. If this site binding is not present, skip these substeps. 5. If this site binding is present, select it and click **Edit.** 6. In the Edit Site Binding window, click **View**. 7. Read the values in the **Issued to:** and **Issued by:** fields. If these values are the same, the computer has a self-signed certificate. If these values are different, the computer has a purchased certificate from a CA. 8. On the Certificate window, click **Details**. 9. Read the value for the signature hash algorithm. If the value is not **sha256**, you need to update your certificate. a. If you have a self-signed certificate, or have a purchased one from a CA that does not need to be updated, make no changes. b. If you need to update a purchased certificate, make no changes, and contact your public CA for how to update your signed certificate to SHA256. If you continue with server installation now, a self-signed certificate is installed, which you can replace with a purchased certificate after the upgrade. 10. Close IIS Manager.

Table 21: Upgrading Unified Metasys Server on Desktop Computer (In-Place)

Step	Action	Reference or Additional Steps
3.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
4.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
5.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
6.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
7.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
8.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.

Table 21: Upgrading Unified Metasys Server on Desktop Computer (In-Place)

Step	Action	Reference or Additional Steps
9.	Uninstall the Ready Access Portal software if currently installed.	Refer to the *Uninstalling Ready Access Portal Software* section in the *Ready Access Portal Software Installation Instructions (LIT-12011523)*.
10.	Uninstall the NxE Information and Configuration Tool (NCT) if present.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
11.	Uninstall the Metasys Export Utility software if currently installed.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
12.	Select the appropriate action: • If Metasys UI Online Release 1.5.1 or earlier software is installed, uninstall Metasys UI Online. • If Metasys UI Online Release 2.0 or higher is installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
13.	Select the appropriate action: • If Metasys UI Offline Release 1.5.1 or earlier software is installed, uninstall Metasys UI Offline. • If Metasys UI Offline Release 2.0 is installed, or Metasys UI Offline is not installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
14.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the current version of Metasys Launcher from the ADS/ADX computer and remove from all clients that log in to the ADS/ADX. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.
15.	Select the appropriate action: • If the computer has ADS/ADX software at Release 7.x or earlier, uninstall the existing ADS/ADX software. When prompted, select to **remove** license keys because you are upgrading to a new major software release. • If the computer has ADS/ADX software at Release 8.x or later, skip to the next step.	See Uninstalling the Metasys Server Software Introduction.

Table 21: Upgrading Unified Metasys Server on Desktop Computer (In-Place)

Step	Action	Reference or Additional Steps
16.	Verify that the currently installed version of SQL Server software is supported for the new release of Metasys software. If necessary, apply the supported service pack or cumulative update.	See Verifying your computer has a supported version of SQL Server software installed.
17.	Uninstall the Metasys Database Manager if currently installed.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
18.	If you uninstalled ADS/ADX software in a previous step because the site was at Release 7.x or earlier, install the Metasys Server 11.0 software now. Otherwise, upgrade the Metasys Server 11.0 software now.	To install, see Metasys Server Software. To upgrade, see Upgrading Metasys Server.
19.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
20.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
21.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
22.	Log on SCT 14.0 with a commissioning laptop, then use the Manage Archive wizard to upgrade the ADS/ADX device to Release 11.0. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If during the upgrade process an Upgrade Warning dialog box appears regarding password resets, set a default password for the affected users, then contact the users of their new default password. Each affected user is prompted to change this default password when logging on the Metasys ADS/ADX Release 11.0 for the first time.	Refer to *Metasys SCT Help (LIT-12011964)*.
23.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.

Table 21: Upgrading Unified Metasys Server on Desktop Computer (In-Place)

Step	Action	Reference or Additional Steps
24.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
25.	Install the Metasys Database Manager to Release 11.0. Metasys Database Manager and the Metasys Server software must be at the same release.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
26.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.
27.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.

Table 21: Upgrading Unified Metasys Server on Desktop Computer (In-Place)

Step	Action	Reference or Additional Steps
28.	If you need to bind a purchased SHA256 certificate from a public certificate authority, follow the steps on the right. ⓘ **Note:** The purchased certificate must be SHA256 to work with Metasys UI.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start Internet Information Services (IIS) Manager. 3. Expand the server, then expand Sites. 4. Click **Default Web Site**. 5. Click **Bindings** in the right pane. The Site Bindings window appears. 6. Select the Site Binding called **Type: https, Port: 443**. 7. Click **Edit.** The Edit Site Binding window appears with the SSL certificate drop-down list currently showing **MUI Application Server**. Click **Select** and select your signed certificate on the Select Certificate window. 8. Click **OK** to confirm your selection, then click **OK** on the Edit Site Binding window. 9. Close all windows.
29.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
30.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading Unified Metasys Server on Server OS

Table 22: Supported Platforms Unified Metasys Server on Server OS

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for upgrading the Metasys Server software on a computer with a server operating system.

Table 23: Upgrading Unified Metasys Server on Server OS (In-Place)

Step	Action	Reference or Additional Steps
1.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
2.	Check if the computer has a SHA256 self-signed certificate bound to Default Web Site in IIS. If the ADS/ADX computer has a purchased certificate from a certificate authority (CA), determine if this is a SHA256 (Secure Hash Algorithm) certificate. If so, follow the steps on the right. If not, skip to the next step. Also, for more details, refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start IIS Manager. Expand the server, then expand Sites. 3. Click **Default Web Site**. Click **Bindings** in the right pane. The Site Bindings window appears. 4. Look for a Site Binding called **Type: https, Port: 443**. If this site binding is not present, skip these substeps. 5. If this site binding is present, select it and click **Edit.** 6. In the Edit Site Binding window, click **View**. 7. Read the values in the **Issued to:** and **Issued by:** fields. If these values are the same, the computer has a self-signed certificate. If these values are different, the computer has a purchased certificate from a CA. 8. On the Certificate window, click **Details**. 9. Read the value for the signature hash algorithm. If the value is not **sha256**, you need to update your certificate. a. If you have a self-signed certificate, or have a purchased one from a CA that does not need to be updated, make no changes. b. If you need to update a purchased certificate, make no changes, and contact your public CA for how to update your signed certificate to SHA256. If you continue with server installation now, a self-signed certificate is installed, which you can replace with a purchased certificate after the upgrade. 10. Close IIS Manager.

Table 23: Upgrading Unified Metasys Server on Server OS (In-Place)

Step	Action	Reference or Additional Steps
3.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
4.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
5.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
6.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
7.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
8.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.

Table 23: Upgrading Unified Metasys Server on Server OS (In-Place)

Step	Action	Reference or Additional Steps
9.	Uninstall the Ready Access Portal software if currently installed.	Refer to the *Uninstalling Ready Access Portal Software* section in the *Ready Access Portal Software Installation Instructions (LIT-12011523)*.
10.	Uninstall the NxE Information and Configuration Tool (NCT) if present.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
11.	Uninstall the Metasys Export Utility software if currently installed.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
12.	Uninstall Energy Essentials if present. This uninstall step is required before you uninstall the ADS/ADX software in a later step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
13.	Select the appropriate action: • If Metasys UI Online Release 1.5.1 or earlier software is installed, uninstall Metasys UI Online. • If Metasys UI Online Release 2.0 or higher is installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
14.	Select the appropriate action: • If Metasys UI Offline Release 1.5.1 or earlier software is installed, uninstall Metasys UI Offline. • If Metasys UI Offline Release 2.0 is installed, or Metasys UI Offline is not installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
15.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the current version of Metasys Launcher from the ADS/ADX computer and remove from all clients that log in to the ADS/ADX. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.
16.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the NAE Update Tool if present. This uninstall step is required before you can install or upgrade to the new version of SCT. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.

Table 23: Upgrading Unified Metasys Server on Server OS (In-Place)

Step	Action	Reference or Additional Steps
17.	Uninstall the existing MVE software if present.	See Uninstalling MVE Software.
18.	Select the appropriate action: • If the computer has ADS/ADX software at Release 7.x or earlier, uninstall the existing ADS/ADX software. When prompted, select to **remove** license keys because you are upgrading to a new major software release. • If the computer has ADS/ADX software at Release 8.x or later, skip to the next step.	See Uninstalling the Metasys Server Software Introduction.
19.	Verify that the currently installed version of SQL Server software is supported for the new release of Metasys software. If necessary, apply the supported service pack or cumulative update.	See Verifying your computer has a supported version of SQL Server software installed.
20.	If you intend to use the Metasys Advanced Reporting System or Energy Essentials, verify that Reporting Services is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
21.	Install support files if the job site requires Metasys software in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
22.	Uninstall the Metasys Database Manager if currently installed.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
23.	If you uninstalled ADS/ADX software in a previous step because the site was at Release 7.x or earlier, install the Metasys Server 11.0 software now. Otherwise, upgrade the Metasys Server 11.0 software now.	To install, see Metasys Server Software. To upgrade, see Upgrading Metasys Server.
24.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
25.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
26.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.

Table 23: Upgrading Unified Metasys Server on Server OS (In-Place)

Step	Action	Reference or Additional Steps
27.	Log on SCT 14.0 with a commissioning laptop, then use the Manage Archive wizard to upgrade the ADS/ADX device to Release 11.0. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If during the upgrade process an Upgrade Warning dialog box appears regarding password resets, set a default password for the affected users, then contact the users of their new default password. Each affected user is prompted to change this default password when logging on the Metasys ADS/ADX Release 11.0 for the first time.	Refer to *Metasys SCT Help (LIT-12011964)*.
28.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
29.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
30.	Install the Metasys Database Manager to Release 11.0. Metasys Database Manager and the Metasys Server software must be at the same release.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
31.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.

Table 23: Upgrading Unified Metasys Server on Server OS (In-Place)

Step	Action	Reference or Additional Steps
32.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
33.	If you need to bind a purchased SHA256 certificate from a public certificate authority, follow the steps on the right. ⓘ **Note:** The purchased certificate must be SHA256 to work with Metasys UI.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start Internet Information Services (IIS) Manager. 3. Expand the server, then expand Sites. 4. Click **Default Web Site**. 5. Click **Bindings** in the right pane. The Site Bindings window appears. 6. Select the Site Binding called **Type: https, Port: 443**. 7. Click **Edit.** The Edit Site Binding window appears with the SSL certificate drop-down list currently showing **MUI Application Server**. Click **Select** and select your signed certificate on the Select Certificate window. 8. Click **OK** to confirm your selection, then click **OK** on the Edit Site Binding window. 9. Close all windows.
34.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
35.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading Unified Metasys Server and SCT on Desktop OS

Table 24: Supported Platforms Unified Metasys Server on Desktop OS with SCT

Supported Operating System	Supported Database Options
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	SQL Server® 2019 Express (64-bit) SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)

Use the steps in the following table for upgrading the Metasys Server and SCT software on a computer with a desktop operating system.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
1.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
2.	Check if the computer has a SHA256 self-signed certificate bound to Default Web Site in IIS. If the ADS/ADX computer has a purchased certificate from a certificate authority (CA), determine if this is a SHA256 (Secure Hash Algorithm) certificate. If so, follow the steps on the right. If not, skip to the next step. Also, for more details, refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start IIS Manager. Expand the server, then expand Sites. 3. Click **Default Web Site**. Click **Bindings** in the right pane. The Site Bindings window appears. 4. Look for a Site Binding called **Type: https, Port: 443**. If this site binding is not present, skip these substeps. 5. If this site binding is present, select it and click **Edit.** 6. In the Edit Site Binding window, click **View**. 7. Read the values in the **Issued to:** and **Issued by:** fields. If these values are the same, the computer has a self-signed certificate. If these values are different, the computer has a purchased certificate from a CA. 8. On the Certificate window, click **Details**. 9. Read the value for the signature hash algorithm. If the value is not **sha256**, you need to update your certificate. a. If you have a self-signed certificate, or have a purchased one from a CA that does not need to be updated, make no changes. b. If you need to update a purchased certificate, make no changes, and contact your public CA for how to update your signed certificate to SHA256. If you continue with server installation now, a self-signed certificate is installed, which you can replace with a purchased certificate after the upgrade. 10. Close IIS Manager.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
3.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
4.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
5.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
6.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
7.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
8.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
9.	Uninstall the Ready Access Portal software if currently installed.	Refer to the *Uninstalling Ready Access Portal Software* section in the *Ready Access Portal Software Installation Instructions (LIT-12011523)*.
10.	Uninstall the NxE Information and Configuration Tool (NCT) if present.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
11.	Uninstall the Metasys Export Utility software if currently installed.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
12.	Select the appropriate action: • If Metasys UI Online Release 1.5.1 or earlier software is installed, uninstall Metasys UI Online. • If Metasys UI Online Release 2.0 or higher is installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
13.	Select the appropriate action: • If Metasys UI Offline Release 1.5.1 or earlier software is installed, uninstall Metasys UI Offline. • If Metasys UI Offline Release 2.0 is installed, or Metasys UI Offline is not installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
14.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the NAE Update Tool if present. This uninstall step is required before you can install or upgrade to the new version of SCT. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
15.	Select the appropriate action: • If the computer has ADS/ADX software at Release 7.x or earlier, uninstall the existing ADS/ADX software. When prompted, select to **remove** license keys because you are upgrading to a new major software release. • If the computer has ADS/ADX software at Release 8.x or later, skip to the next step.	See Uninstalling the Metasys Server Software Introduction.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
16.	Select the appropriate action: • If you have **SCT Release 7.x to 10.x or SCT 11.1 to 13.x**, skip to the next step. • If you have **SCT Release 6.5.x or earlier, or SCT 11.0**, follow the steps to the right to manually record all SCT users.	1. Log in to SCT and open the Security Administrator tool (**Tools > Administrator**). 2. In Security Administrator, record all SCT roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All SCT customized roles and user accounts are lost when you uninstall SCT in the next step. 3. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role.
17.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the current version of Metasys Launcher from the ADS/ADX computer and remove from all clients that log in to the ADS/ADX. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.
18.	Verify that the currently installed version of SQL Server software is supported for the new release of Metasys software. If necessary, apply the supported service pack or cumulative update.	See Verifying your computer has a supported version of SQL Server software installed.
19.	Select the appropriate action: • If you have **SCT Release 6.5.x or earlier**, skip to the next step. • If you have **SCT Release 7.0 to 13.1**, follow the steps to the right. • If you have **SCT Release 13.2 or 13.3**, upgrade to SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.	1. Uninstall the existing SCT 7.0 to SCT 13.1 software. To retain the SCT security database, make sure that you **uncheck** the box for removing databases. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
20.	Select the appropriate action: • If you have **SCT Release 7.0 or later**, skip to the next step. • If you have **SCT Release 6.5.x or earlier**, follow the steps to the right.	1. Uninstall the existing SCT 6.5.x or earlier software. The SCT and ADS/ADX security databases are not separate at Release 6.5.x or earlier, so an SCT upgrade option is not available. Refer to the *Uninstalling SCT* section of the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install and license the SCT 14.0 software. Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
21.	Start SCT from the Launcher or the Metasys SCT shortcut. Log in with the MetasysSysAgent user and password. The login process could take a little longer than usual.	Refer to *Launcher Tool Help (LIT-12011742)*.
22.	As part of the in-place upgrade, open the archive database with SCT by clicking **Item > Open Archive**. See the information on the right.	Select the appropriate action: • If the archive database is not listed, use SCT to restore the database (**Tools > Database > Restore Backup**). After the restore completes, open the archive by clicking **Item > Open Archive**. Click **Upgrade** to upgrade the archive to the new release. • A message to upgrade the archive to this Metasys system release appears. Click **Upgrade Archive** to upgrade the archive to the new release.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
23.	Select the appropriate action: • If you upgraded SCT from **Release 7.x or Release 11.1** to Release 14.0, go on to the next step. • If you upgraded SCT from **Release 6.5.x or earlier, or Release 11.0** to Release 14.0, start SCT. Open the Security Administrator tool (Tools > Administrator). In Security Administrator, recreate all roles, user accounts, and Active Directory user accounts that were present in the old version of SCT (or, create a new limited set of SCT users). If you made screen captures of the SCT roles and users in an earlier step, use these screens as a guide for adding the roles and user accounts to SCT.	Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
24.	Uninstall the Metasys Database Manager if currently installed.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
25.	If you uninstalled ADS/ADX software in a previous step because the site was at Release 7.x or earlier, install the Metasys Server 11.0 software now. Otherwise, upgrade the Metasys Server 11.0 software now.	To install, see Metasys Server Software. To upgrade, see Upgrading Metasys Server.
26.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
27.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
28.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
29.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.
30.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
31.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
32.	As part of the in-place upgrade, install the Metasys Database Manager at Release 11.0.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
33.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.

Table 25: Upgrading Unified Metasys Server with SCT on Desktop OS (In-Place)

Step	Action	Reference or Additional Steps
34.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
35.	If you need to bind a purchased SHA256 certificate from a public certificate authority, follow the steps on the right. ⓘ **Note:** The purchased certificate must be SHA256 to work with Metasys UI.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start Internet Information Services (IIS) Manager. 3. Expand the server, then expand Sites. 4. Click **Default Web Site**. 5. Click **Bindings** in the right pane. The Site Bindings window appears. 6. Select the Site Binding called **Type: https, Port: 443**. 7. Click **Edit.** The Edit Site Binding window appears with the SSL certificate drop-down list currently showing **MUI Application Server**. Click **Select** and select your signed certificate on the Select Certificate window. 8. Click **OK** to confirm your selection, then click **OK** on the Edit Site Binding window. 9. Close all windows.
36.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading Unified Metasys Server and SCT on Server OS

Table 26: Supported Platforms Unified Metasys Server with SCT Server OS

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for upgrading the Metasys Server and SCT software on a computer with a server operating system.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
1.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
2.	Check if the computer has a SHA256 self-signed certificate bound to Default Web Site in IIS. If the ADS/ADX computer has a purchased certificate from a certificate authority (CA), determine if this is a SHA256 (Secure Hash Algorithm) certificate. If so, follow the steps on the right. If not, skip to the next step. Also, for more details, refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start IIS Manager. Expand the server, then expand Sites. 3. Click **Default Web Site**. Click **Bindings** in the right pane. The Site Bindings window appears. 4. Look for a Site Binding called **Type: https, Port: 443**. If this site binding is not present, skip these substeps. 5. If this site binding is present, select it and click **Edit.** 6. In the Edit Site Binding window, click **View**. 7. Read the values in the **Issued to:** and **Issued by:** fields. If these values are the same, the computer has a self-signed certificate. If these values are different, the computer has a purchased certificate from a CA. 8. On the Certificate window, click **Details**. 9. Read the value for the signature hash algorithm. If the value is not **sha256**, you need to update your certificate. a. If you have a self-signed certificate, or have a purchased one from a CA that does not need to be updated, make no changes. b. If you need to update a purchased certificate, make no changes, and contact your public CA for how to update your signed certificate to SHA256. If you continue with server installation now, a self-signed certificate is installed, which you can replace with a purchased certificate after the upgrade. 10. Close IIS Manager.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
3.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
4.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
5.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
6.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
7.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
8.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
9.	Uninstall the Ready Access Portal software if currently installed.	Refer to the *Uninstalling Ready Access Portal Software* section in the *Ready Access Portal Software Installation Instructions (LIT-12011523)*.
10.	Uninstall the NxE Information and Configuration Tool (NCT) if present.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
11.	Uninstall the Metasys Export Utility software if currently installed.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
12.	Uninstall Energy Essentials if present. This uninstall step is required before you uninstall the ADS/ADX software in a later step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
13.	Select the appropriate action: • If Metasys UI Online Release 1.5.1 or earlier software is installed, uninstall Metasys UI Online. • If Metasys UI Online Release 2.0 or higher is installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
14.	Select the appropriate action: • If Metasys UI Offline Release 1.5.1 or earlier software is installed, uninstall Metasys UI Offline. • If Metasys UI Offline Release 2.0 is installed, or Metasys UI Offline is not installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
15.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the NAE Update Tool if present. This uninstall step is required before you can install or upgrade to the new version of SCT. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
16.	Uninstall the existing MVE software if present.	See Uninstalling MVE Software.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
17.	Select the appropriate action: • If the computer has ADS/ADX software at Release 7.x or earlier, uninstall the existing ADS/ADX software. When prompted, select to **remove** license keys because you are upgrading to a new major software release. • If the computer has ADS/ADX software at Release 8.x or later, skip to the next step.	See Uninstalling the Metasys Server Software Introduction.
18.	Select the appropriate action: • If you have **SCT Release 7.x to 10.x or SCT 11.1 to 13.x**, skip to the next step. • If you have **SCT Release 6.5.x or earlier, or SCT 11.0**, follow the steps to the right to manually record all SCT users.	1. Log in to SCT and open the Security Administrator tool (**Tools > Administrator**). 2. In Security Administrator, record all SCT roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All SCT customized roles and user accounts are lost when you uninstall SCT in the next step. 3. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role.
19.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the current version of Metasys Launcher from the ADS/ADX computer and remove from all clients that log in to the ADS/ADX. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.
20.	Select the appropriate action: • If you have **SCT Release 6.5.x or earlier**, skip to the next step. • If you have **SCT Release 7.0 to 13.1**, follow the steps to the right. • If you have **SCT Release 13.2 or 13.3**, upgrade to SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.	1. Uninstall the existing SCT 7.0 to SCT 13.1 software. To retain the SCT security database, make sure that you **uncheck** the box for removing databases. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
21.	Select the appropriate action: • If you have **SCT Release 7.0 or later**, skip to the next step. • If you have **SCT Release 6.5.x or earlier**, follow the steps to the right.	1. Uninstall the existing SCT 6.5.x or earlier software. The SCT and ADS/ADX security databases are not separate at Release 6.5.x or earlier, so an SCT upgrade option is not available. Refer to the *Uninstalling SCT* section of the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install and license the SCT 14.0 software. Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
22.	Start SCT from the Launcher or the Metasys SCT shortcut. Log in with the MetasysSysAgent user and password. The login process could take a little longer than usual.	Refer to *Launcher Tool Help (LIT-12011742)*.
23.	As part of the in-place upgrade, open the archive database with SCT by clicking **Item > Open Archive**. See the information on the right.	Select the appropriate action: • If the archive database is not listed, use SCT to restore the database (**Tools > Database > Restore Backup**). After the restore completes, open the archive by clicking **Item > Open Archive**. Click **Upgrade** to upgrade the archive to the new release. • A message to upgrade the archive to this Metasys system release appears. Click **Upgrade Archive** to upgrade the archive to the new release.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
24.	Select the appropriate action: • If you upgraded SCT from **Release 7.x or Release 11.1** to Release 14.0, go on to the next step. • If you upgraded SCT from **Release 6.5.x or earlier, or Release 11.0** to Release 14.0, start SCT. Open the Security Administrator tool (Tools > Administrator). In Security Administrator, recreate all roles, user accounts, and Active Directory user accounts that were present in the old version of SCT (or, create a new limited set of SCT users). If you made screen captures of the SCT roles and users in an earlier step, use these screens as a guide for adding the roles and user accounts to SCT.	Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
25.	Uninstall the Metasys Database Manager if currently installed.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
26.	If you uninstalled ADS/ADX software in a previous step because the site was at Release 7.x or earlier, install the Metasys Server 11.0 software now. Otherwise, upgrade the Metasys Server 11.0 software now.	To install, see Metasys Server Software. To upgrade, see Upgrading Metasys Server.
27.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
28.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
29.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
30.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.
31.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
32.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
33.	As part of the in-place upgrade, install the Metasys Database Manager at Release 11.0.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
34.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.

Table 27: Upgrading Unified Metasys Server with SCT on Server Computer (In-Place)

Step	Action	Reference or Additional Steps
35.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
36.	If you need to bind a purchased SHA256 certificate from a public certificate authority, follow the steps on the right. ⓘ **Note:** The purchased certificate must be SHA256 to work with Metasys UI.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start Internet Information Services (IIS) Manager. 3. Expand the server, then expand Sites. 4. Click **Default Web Site**. 5. Click **Bindings** in the right pane. The Site Bindings window appears. 6. Select the Site Binding called **Type: https, Port: 443**. 7. Click **Edit.** The Edit Site Binding window appears with the SSL certificate drop-down list currently showing **MUI Application Server**. Click **Select** and select your signed certificate on the Select Certificate window. 8. Click **OK** to confirm your selection, then click **OK** on the Edit Site Binding window. 9. Close all windows.
37.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading a Split Metasys Server and SCT

Upgrading a split Metasys system with SCT involves three computers:

- SCT Computer
- Database Server

- Web/Application Server

ⓘ **Note:** Always set up the SCT computer first.

SCT Computer

Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)* for more information on supported platforms and for installing SCT.

Use the steps in the following table for upgrading SCT on a split Metasys system.

Table 28: Upgrading SCT on Different Computer from Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
1.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
2.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
3.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
4.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.

Table 28: Upgrading SCT on Different Computer from Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
5.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
6.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.
7.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
8.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the NAE Update Tool if present. This uninstall step is required before you can install or upgrade to the new version of SCT. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
9.	Uninstall the NxE Information and Configuration Tool (NCT) if present.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
10.	Select the appropriate action: • If you have **SCT Release 7.x to 10.x or SCT 11.1 to 13.x**, skip to the next step. • If you have **SCT Release 6.5.x or earlier, or SCT 11.0**, follow the steps to the right to manually record all SCT users.	1. Log in to SCT and open the Security Administrator tool (**Tools > Administrator**). 2. In Security Administrator, record all SCT roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All SCT customized roles and user accounts are lost when you uninstall SCT in the next step. 3. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role.
11.	Uninstall the current version of Metasys Launcher from the SCT computer and remove from all clients that log in to the ADS/ADX.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.

Table 28: Upgrading SCT on Different Computer from Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
12.	Select the appropriate action: • If you have **SCT Release 6.5.x or earlier**, skip to the next step. • If you have **SCT Release 7.0 to 13.1**, follow the steps to the right. • If you have **SCT Release 13.2 or 13.3**, upgrade to SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.	1. Uninstall the existing SCT 7.0 to SCT 13.1 software. To retain the SCT security database, make sure that you **uncheck** the box for removing databases. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
13.	Select the appropriate action: • If you have **SCT Release 7.0 or later**, skip to the next step. • If you have **SCT Release 6.5.x or earlier**, follow the steps to the right.	1. Uninstall the existing SCT 6.5.x or earlier software. The SCT and ADS/ADX security databases are not separate at Release 6.5.x or earlier, so an SCT upgrade option is not available. Refer to the *Uninstalling SCT* section of the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install and license the SCT 14.0 software. Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
14.	Start SCT from the Launcher or the Metasys SCT shortcut. Log in with the MetasysSysAgent user and password. The login process could take a little longer than usual.	Refer to *Launcher Tool Help (LIT-12011742)*.
15.	As part of the in-place upgrade, open the archive database with SCT by clicking **Item > Open Archive**. See the information on the right.	Select the appropriate action: • If the archive database is not listed, use SCT to restore the database (**Tools > Database > Restore Backup**). After the restore completes, open the archive by clicking **Item > Open Archive**. Click **Upgrade** to upgrade the archive to the new release. • A message to upgrade the archive to this Metasys system release appears. Click **Upgrade Archive** to upgrade the archive to the new release.

Table 28: Upgrading SCT on Different Computer from Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
16.	Select the appropriate action: • If you upgraded SCT from **Release 7.x or Release 11.1** to Release 14.0, go on to the next step. • If you upgraded SCT from **Release 6.5.x or earlier, or Release 11.0** to Release 14.0, start SCT. Open the Security Administrator tool (Tools > Administrator). In Security Administrator, recreate all roles, user accounts, and Active Directory user accounts that were present in the old version of SCT (or, create a new limited set of SCT users). If you made screen captures of the SCT roles and users in an earlier step, use these screens as a guide for adding the roles and user accounts to SCT.	Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
17.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.
18.	Go to the next section to upgrade the database server of the split ADX.	Go to Database Server.

Database Server

Table 29: Supported Platforms Split Metasys Server for Database Server

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for upgrading the database component of the ADX on a split Metasys system.

Table 30: Upgrading Database Server on Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
1.	Verify that the currently installed version of SQL Server software is supported for the new release of Metasys software. If necessary, apply the supported service pack or cumulative update.	See Verifying your computer has a supported version of SQL Server software installed.
2.	Install the Metasys Database Manager to Release 11.0. Metasys Database Manager and the Metasys Server software must be at the same release.	Refer to the *Metasys Database Manager Installation Guide (LIT-12011553)*.
3.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
4.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.
5.	Go to the next section to upgrade the web/application server of the split ADX.	Go to Web/Application Server.

Web/Application Server

Table 31: Supported Platforms Split Metasys Server for Web/Application Server

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Follow these steps to upgrade the web/application component of the ADX on a split Metasys system.

Table 32: Upgrading Web/Application Server on Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
1.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
2.	Check if the computer has a SHA256 self-signed certificate bound to Default Web Site in IIS. If the ADS/ADX computer has a purchased certificate from a certificate authority (CA), determine if this is a SHA256 (Secure Hash Algorithm) certificate. If so, follow the steps on the right. If not, skip to the next step. Also, for more details, refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start IIS Manager. Expand the server, then expand Sites. 3. Click **Default Web Site**. Click **Bindings** in the right pane. The Site Bindings window appears. 4. Look for a Site Binding called **Type: https, Port: 443**. If this site binding is not present, skip these substeps. 5. If this site binding is present, select it and click **Edit.** 6. In the Edit Site Binding window, click **View**. 7. Read the values in the **Issued to:** and **Issued by:** fields. If these values are the same, the computer has a self-signed certificate. If these values are different, the computer has a purchased certificate from a CA. 8. On the Certificate window, click **Details**. 9. Read the value for the signature hash algorithm. If the value is not **sha256**, you need to update your certificate. a. If you have a self-signed certificate, or have a purchased one from a CA that does not need to be updated, make no changes. b. If you need to update a purchased certificate, make no changes, and contact your public CA for how to update your signed certificate to SHA256. If you continue with server installation now, a self-signed certificate is installed, which you can replace with a purchased certificate after the upgrade. 10. Close IIS Manager.

Table 32: Upgrading Web/Application Server on Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
3.	Uninstall the Ready Access Portal software if currently installed.	Refer to the *Uninstalling Ready Access Portal Software* section in the *Ready Access Portal Software Installation Instructions (LIT-12011523)*.
4.	Uninstall the Metasys Export Utility software if currently installed.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
5.	Uninstall Energy Essentials if present. This uninstall step is required before you uninstall the ADS/ADX software in a later step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
6.	Select the appropriate action: • If Metasys UI Online Release 1.5.1 or earlier software is installed, uninstall Metasys UI Online. • If Metasys UI Online Release 2.0 or higher is installed, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
7.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the current version of Metasys Launcher from the ADS/ADX computer and remove from all clients that log in to the ADS/ADX. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.
8.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the NAE Update Tool if present. This uninstall step is required before you can install or upgrade to the new version of SCT. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.
9.	Uninstall the existing MVE software if present.	See Uninstalling MVE Software.

Table 32: Upgrading Web/Application Server on Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
10.	Select the appropriate action: • If the computer has ADS/ADX software at Release 7.x or earlier, uninstall the existing ADS/ADX software. When prompted, select to **remove** license keys because you are upgrading to a new major software release. • If the computer has ADS/ADX software at Release 8.x or later, skip to the next step.	See Uninstalling the Metasys Server Software Introduction.
11.	Restart the computer.	Refer to the information for restarting the computer that came with your operating system.
12.	Verify that the currently installed version of SQL Server software is supported for the new release of Metasys software. If necessary, apply the supported service pack or cumulative update.	See Verifying your computer has a supported version of SQL Server software installed.
13.	Verify that SQL Server Reporting Services is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
14.	If you uninstalled ADS/ADX software in a previous step because the site was at Release 7.x or earlier, install the Metasys Server 11.0 software. Otherwise, upgrade the Metasys Server 11.0 software. When you install or upgrade, specify the SCT archive database in the SCT Archive Db field on the Reporting tab screen of the Metasys Server 10.1 installer. Make sure you install the new Metasys Server 11.0 software on the Site Director first. If you have other ADSs/ADXs, upgrade them after the Site Director.	See Upgrading Metasys Server or Metasys Server Software.
15.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
16.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
17.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.

Table 32: Upgrading Web/Application Server on Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
18.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
19.	If the site has other ADS/ADX servers, upgrade and download each ADS/ADX archive database from SCT 14.0 to the other ADS/ADX servers. The download also restores user accounts.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
20.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
21.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.
22.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine. The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engines (NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.

Table 32: Upgrading Web/Application Server on Split Metasys Server (In-Place)

Step	Action	Reference or Additional Steps
23.	If you need to bind a purchased SHA256 certificate from a public certificate authority, follow the steps on the right. ⓘ **Note:** The purchased certificate must be SHA256 to work with Metasys UI.	1. In Control Panel, click **System and Security** > **Administrative Tools.** 2. Start Internet Information Services (IIS) Manager. 3. Expand the server, then expand Sites. 4. Click **Default Web Site**. 5. Click **Bindings** in the right pane. The Site Bindings window appears. 6. Select the Site Binding called **Type: https, Port: 443**. 7. Click **Edit.** The Edit Site Binding window appears with the SSL certificate drop-down list currently showing **MUI Application Server**. Click **Select** and select your signed certificate on the Select Certificate window. 8. Click **OK** to confirm your selection, then click **OK** on the Edit Site Binding window. 9. Close all windows.
24.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
25.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Metasys Server Out-of-Place Upgrade

This section includes the steps for performing an **out-of-place upgrade** of the ADS or ADX software to Metasys Server 10.1. An out-of-place upgrade applies in either of these two scenarios: (1) you need to reformat the computer that is currently running the Metasys system to a new, supported Windows operating system before performing the upgrade or (2) you need to move the current Metasys system to a different computer or virtual machine during the upgrade. Before upgrading to Metasys Server 10.1 software, make sure you review Pre-Work checklist for new installations and upgrades and Out-of-Place Upgrade Considerations.

Which type of Metasys Server are you upgrading?	
Unified ADS	Select to upgrade a Metasys Server on a **desktop** operating system.
Unified ADS with SCT	Select to upgrade a Metasys Server and SCT on a **desktop** operating system.
Unified ADX	Select to upgrade a Metasys Server on a **server-class** operating system.
Unified ADX with SCT	Select to upgrade a Metasys Server and SCT on a **server-class** operating system.
Split ADX with SCT	Select to upgrade a Metasys Server and SCT on a split configuration. With a split ADX, the database component is installed on one **server-class** system, the web/application component is installed on another **server-class** operating system, and SCT is installed on either a **server-class** or **desktop** operating system.

Out-of-Place Upgrade Considerations

Before starting the out-of-place upgrade process, review the following table.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Current condition of all Metasys system software	Before you start the upgrade, make sure that all currently loaded Metasys software applications are functioning properly. In particular, verify these applications: Metasys Database Manager, Metasys Export Utility, Metasys UI, Metasys Advanced Reporting System (ARS), and Energy Essentials.	Refer to the respective help systems and user guides.
Current version of Windows operating system.	Before you start the upgrade, make sure that the computer you want to use for the Metasys system has a supported operating system. The supported Windows operating system versions are shown to the right.	To verify the Windows operating system, open a command prompt window and run the command **msinfo32**. Verify the version is at this level or higher: **Windows 10:** Version 1903 10.18362 **Windows 8.1:** Version 6.3.9600 **Windows Server 2019:** Version 10.0.118362 **Windows Server 2016**: Version 10.0.14393

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Current Version of Microsoft® SQL Server® Software	If your Metasys system is currently using a version of SQL Server software that is no longer supported, you need to upgrade to a newer version. The Metasys Server installer halts if it detects the currently installed version, service pack, and cumulative update (CU) of SQL Server is not unsupported. For a list of supported SQL Server versions, SPs, and CUs, see Prerequisite Software Checklist for Installation and Upgrade. Also, if you are performing an out-of-place upgrade in which the new computer name is different from the old computer name, you need to update the Site Director and device names in the Metasys system databases. If you are renaming databases prior to SQL Server 2012, contact FSC for additional SQL scripts you need to run prior to following the steps in the *Renaming Field Contents in Metasys Databases* section of the *Metasys Database Manager Help (LIT-12011202)*. You can also refer to FSC Solutions Database article 34534.	See Verifying your computer has a supported version of SQL Server software installed. For more information on installing or upgrading SQL Server software, refer to the *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
Overall Current Condition of HVAC Systems Monitored by Metasys	Run and print out an Alarm summary and Override summary to document any existing system issues.	Refer to *Metasys Site Management Portal Help (LIT-1201793)*.
Windows Event Viewer	Check the Windows Event Viewer for any system, ADS, and MDM error messages.	Consult the Windows operating system documentation.
Available Hard Disk Space	Verify available disk space on the computer or VM that you will use for the Metasys Server. If you need more disk space, try removing any miscellaneous and temporary files.	Consult the Windows operating system documentation.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Security Database	If the current Metasys system is at **Release 5.2 or earlier**, log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. If the current Metasys system is at **Release 6.0 or later**, no separate security database backup is required because the security database is part of the archive database. Backing up the archive backs up security as well.	Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
Archive Database	Using the existing release of SCT, upload the archive database, making sure you select the Include Security option. Then, create a database backup of the archive. Also create an export of the database with SCT. Backups are found in C:\ProgramData\Johnson Controls\MetasysIII\DatabaseFiles	*Upload*, *Backing Up an Archive Database*, and *Export Database* sections of the *Metasys SCT Help (LIT-12011964)*.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
User Accounts and Passwords	Gather any applicable administrator user names and passwords that are required for installing or upgrading software. This includes the SQL System Administrator (sa) account and password. For customers who do not want to share these credentials, arrange for the SQL DBA to assist. Alternatively, the DBA can create a temporary SQL admin account with SA privileges just for the installation of the software, which can be removed later.	Consult the customer's IT administration.
User accounts with passwords that have not been recently modified or were created with an older release of Metasys that had different password requirements	To comply with the FIPS 140-2 standard, security changes to passwords were made at Metasys Release 11.0. At Release 8.1 and earlier, passwords were stored in a SHA1-hashed format, which is not FIPS compliant. Therefore, if you are upgrading your Metasys system from Release 8.1 or earlier, passwords of user accounts are reset with a default password that you specify during the archive upgrade process. To prevent user lock out for existing users, verify that the Never Expire property under Account Policy is not set. Additionally, set a new password for any user who has not changed their password in more than two years.	*Security Administrator System Technical Bulletin (LIT-1201528)*

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Basic access user accounts	Basic access users and the BasicSysAgent user account are no longer available at Release 11.0. The BasicSysAgent account is removed and all users with Basic access are converted to Standard access users when you upgrade the archive to SCT Release 14.0.	*Security Administrator System Technical Bulletin (LIT-1201528)*
RADIUS user accounts	RADIUS user accounts are no longer supported at Release 11.0. During the database archive upgrade process with SCT 14.0, each RADIUS user account in the archive is converted to a Metasys local user with an undefined password and a locked account. To activate the converted RADIUS account, a Metasys user with Administrator rights sets an initial password and unlocks the account.	*Security Administrator System Technical Bulletin (LIT-1201528)*
Preferences	Save your preference files to a safe location **before** the upgrade. You can move the files to the appropriate location on the new computer after the upgrade is complete. The preferences you need to save might include special alarm sound files and color selections, startup views, and links to external applications. Beginning with SCT 11.0, the upload and download processes include user preferences. However, SCT does not upload user preferences from a Site Director NAE.	Refer to the *Configuring and Maintaining Preferences Appendix* of the *ADS/ADX Commissioning Guide (LIT-1201645)* or the *NAE Commissioning Guide (LIT-1201519)*.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Object Lists	Object lists stored in network engines do not persist during an upgrade to Release 11.0. Object lists are saved as files by the Global Search feature when you save search results. Save your object list files to a safe location **before** the upgrade. You can move the files to the appropriate location on the new computer after the upgrade is complete. Beginning with SCT 11.0, the upload and download processes include the object lists. However, SCT does not upload object lists from a Site Director NAE.	Refer to the *Configuring and Maintaining Preferences Appendix* of the *ADS/ADX Commissioning Guide (LIT-1201645)* or the *NAE Commissioning Guide (LIT-1201519)*.
Customized Config or Properties Files[1]	If you have customized files for your system, be sure to note those customizations before you upgrade. After the upgrade, be sure to reapply your custom settings to the new computer. ⓘ **Note:** When upgrading, do not replace the new file with a copy of the old file. Other settings in the file may have been changed to improve system performance or support new features. **Instead of replacing the new file with a copy of the old one, reapply the custom settings in the new file.**	Documentation for each specific product covers customization procedures; or, you may be directed to update files by support personnel.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Historical Data	Install the Metasys Database Manager on the Metasys Server if it is not already present. Then, a few hours before you plan the system upgrade (so as to not lose too much data), use Metasys Database Manager to back up the historical databases, which include audit (JCIAuditTrails), alarm (JCIEvents), trend (JCIHistorianDB), annotation (JCIItemAnnotation), *Metasys* UI trends (JCIReportingDB), Metasys UI Spaces Authorization (SpacesAuthorization), and reporting system (MetasysReporting). We recommend that you select the reindexing option, even though it significantly increases the length of time for this process. ⓘ **Note:** If the existing system is allowed to run post database backup, there will be gaps in the historical data from when the backup is completed until when the databases are migrated to the new server and it is brought online.	Refer to the *Backing Up a Database* section of the *Metasys Database Manager Help (LIT-12011202)*.
Metasys UI Spaces Authorization (SpacesAuthorization)	If upgrading from Metasys Release 8.0 or 8.1, use SQL Server Management Studio to back up the SpacesAuthorization database because the backup operation for that database is not available with Metasys Database Manager Release 8.0 or 8.1.	Consult the SQL Server Management Studio documentation.
Coexisting versions of Metasys Server and SCT software.	The Metasys Server 11.0 may coexist on the same computer as SCT 14.0.	Refer to *SCT Installation and Upgrade Instructions (LIT-12012067)*.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
License deactivation before out-of-place upgrade (Release 10.0 or later only)	If you are performing an out-of-place upgrade from Release 10.0 or later, be sure to deactivate the Metasys Server license with Software Manager **before** you decommission the old computer or VM. If you skip this step, the license is still active on the old server, which prevents Software Manager from transferring the license to the new server.	Refer to the *License Deactivation Overview* section in *Software Manager Help (LIT-12012389)*.
BACnet Encoding Type	The archive upgrade process changes the BACnet Encoding Type attribute under the Site object. When a site is upgraded to Release 11.0 with SCT 14.0, the BACnet Encoding Type for the Site object is automatically changed to ISO 10646 UTF-8 during the archive upgrade process. If you require UCS-2 as the BACnet Encoding Type, make sure you set this attribute back to **UCS-2** after the archive upgrade is complete.	Refer to Site Object - Attributes section of *Metasys SMP Help (LIT--1201793)*.

Table 33: Upgrade Considerations (Out-of-Place)

Data or Item	Details	Reference
Device pairing	At Metasys Release 10.0, a more secure authentication process was implemented between updated NxEs and the Site Director that involves device pairing. This capability is controlled by a new attribute in the Site object called **Advanced Security Enabled**. If you upgrade to Release 11.0 from an older release, Advanced Security Enabled is defaulted to **True** and NxEs become unpaired with their Site Directors.	Before upgrading to Release 11.0 (or before upgrading to a new build of Release 11.0), follow these steps: 1. Pair all network engines to the Metasys Server. 2. Using SCT, upload the Metasys Server with security to save the pairing information to the archive. 3. Perform the Metasys Server upgrade, but do not update the engines. 4. Using SCT, perform a Security Copy to the newly upgraded Metasys Server. 5. Verify all engines are now paired.

[1] The .config files contain custom Metasys network settings for features including serial printing Destination Delivery Agent (DDA) settings for an NAE, the Metasys Advanced Reporting System ADX, and the Action Queue in SCT. Examples of .config files you may have customized include web.config and ActionQueue.exe.config. Properties files also contain information related to name resolution and other system settings.

Upgrading Unified Metasys Server on Desktop OS

Table 34: Supported Platforms Unified Metasys Server on Desktop OS

Supported Operating System	Supported Database Options
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	SQL Server® 2019 Express (64-bit) SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)

Use the steps in the following table to perform an out-of-place upgrade of Metasys Server software on a computer with a desktop operating system. These steps presume that the computer currently has no Metasys software installed.

Table 35: Upgrading Unified Metasys Server on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software has one of the following supported Windows desktop operating systems: • Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. • Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows 10 with Creators Update: Version 1903 10.18362 • Windows 8.1 with Update 1: Version 6.3.9600 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	If you are installing the Metasys Server software on an English language computer, skip to the next step. If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 35: Upgrading Unified Metasys Server on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. The Server Manager window appears. Use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
8.	Install a version of SQL Server Express software on the computer that the *Metasys* system supports.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
9.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
10.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.
11.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.

Table 35: Upgrading Unified Metasys Server on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
12.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
13.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
14.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.

Table 35: Upgrading Unified Metasys Server on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
15.	As part of performing an out-of-place upgrade, follow the steps to the right.	1. Disconnect the old ADS/ADX computer from the building network. 2. Connect the new ADS/ADX computer to the building network. 3. On the new ADS/ADX computer, assign the same computer name and IP address as the old ADS/ADX computer (**case sensitive**). 4. Install the Metasys Database Manager (Release 11.0) on the new ADS/ADX computer. 5. Copy the Metasys database backup files (.bak) from the old ADS/ADX computer to the Metasys Database Manager Backup folder of the new computer. 6. Copy the SCT archive backup file (.backup) from the old ADS/ADX computer to the new ADS/ADX computer. Place the archive here: `C:\ProgramData\Johnson Controls\MetasysIII\DatabaseFiles`. 7. Start SCT on the new ADS/ADX computer. With SCT, restore the archive backup you copied in the previous step. 8. If the new computer name is different from the old ADS/ADX computer, open the restored SCT archive, upgrade the archive, then rename the Site Director in the upgraded archive to match the new computer name (**case sensitive**). 9. Start the Metasys Database Manager in Expert mode and restore each database backup from the SQLData backup folder. 10. If the new computer name is different from the old ADS/ADX computer, update the Site Director and device names in the Metasys system databases.
16.	Install the Metasys Server 11.0 software.	See Metasys Server Software.
17.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
18.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.

Table 35: Upgrading Unified Metasys Server on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
19.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
20.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.
21.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
22.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
23.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.

Table 35: Upgrading Unified Metasys Server on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
24.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
25.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
26.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading Unified Metasys Server on Server OS

Table 36: Supported Platforms Unified Metasys Server on Server OS

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table to perform an out-of-place upgrade of Metasys Server software on a computer with a server operating system. These steps presume that the computer currently has no Metasys software installed.

Table 37: Upgrading Unified Metasys Server on Server OS (Out-of-Place)

Step	Action	Reference or Step
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	If you are installing the Metasys Server software on an English language computer, skip to the next step. If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 37: Upgrading Unified Metasys Server on Server OS (Out-of-Place)

Step	Action	Reference or Step
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. The Server Manager window appears. Use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
8.	Install a version of SQL Server Standard or Enterprise software on the computer that the *Metasys* system supports. Install these components: Database Engine Services, Reporting Services, and Management Tools.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
9.	Verify that Reporting Services on the computer is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
10.	Install support files on the computer if you plan to offer the Site Management Portal in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
11.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
12.	Determine if you need to record existing user accounts and roles: • If the current Metasys system is at **Release 5.2 and earlier**, follow the steps on the right. • If the current Metasys system is at **Release 6.0 or later**, skip to the next step.	Log in to SCT and open the Security Administrator tool (**Tools** > **Administrator**). In Security Administrator, record all roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All customized roles and user accounts are lost when you uninstall SCT 5.2 (or earlier) and install a newer version of SCT. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role. Refer to the *Metasys Site Management Portal Help (LIT-1201793)* for Release 5.2 or earlier.

Table 37: Upgrading Unified Metasys Server on Server OS (Out-of-Place)

Step	Action	Reference or Step
13.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
14.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
15.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
16.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.
17.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Table 37: Upgrading Unified Metasys Server on Server OS (Out-of-Place)

Step	Action	Reference or Step
18.	As part of performing an out-of-place upgrade, follow the steps to the right.	1. Disconnect the old ADS/ADX computer from the building network. 2. Connect the new ADS/ADX computer to the building network. 3. On the new ADS/ADX computer, assign the same computer name and IP address as the old ADS/ADX computer (**case sensitive**). 4. Install the Metasys Database Manager (Release 11.0) on the new ADS/ADX computer. 5. Copy the Metasys database backup files (.bak) from the old ADS/ADX computer to the Metasys Database Manager Backup folder of the new computer. 6. Copy the SCT archive backup file (.backup) from the old ADS/ADX computer to the new ADS/ADX computer. Place the archive here: `C:\ProgramData\Johnson Controls\MetasysIII\DatabaseFiles`. 7. Start SCT on the new ADS/ADX computer. With SCT, restore the archive backup you copied in the previous step. 8. If the new computer name is different from the old ADS/ADX computer, open the restored SCT archive, upgrade the archive, then rename the Site Director in the upgraded archive to match the new computer name (**case sensitive**). 9. Start the Metasys Database Manager in Expert mode and restore each database backup from the SQLData backup folder. 10. If the new computer name is different from the old ADS/ADX computer, update the Site Director and device names in the Metasys system databases.
19.	Install the Metasys Server 11.0 software.	See Metasys Server Software.
20.	License the Metasys ADS or Metasys ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
21.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.

Table 37: Upgrading Unified Metasys Server on Server OS (Out-of-Place)

Step	Action	Reference or Step
22.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
23.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.
24.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
25.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
26.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.

Table 37: Upgrading Unified Metasys Server on Server OS (Out-of-Place)

Step	Action	Reference or Step
27.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
28.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
29.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading Unified Metasys Server and SCT on Desktop OS

Table 38: Supported Platforms Unified Metasys Server on Desktop OS with SCT

Supported Operating System	Supported Database Options
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support.	SQL Server® 2019 Express (64-bit) SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	SQL Server® 2017 Express with CU17 (64-bit) SQL Server® 2016 Express with SP2 CU10 (64-bit) SQL Server® 2014 Express with SP3 CU4 (64-bit)

Use the steps in the following table to perform an out-of-place upgrade of Metasys Server and SCT software on a computer with a desktop operating system. These steps presume that the computer currently has no Metasys software installed.

Table 39: Upgrading Unified Metasys Server with SCT on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software has one of the following supported Windows desktop operating systems: • Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. • Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows 10 with Creators Update: Version 1903 10.18362 • Windows 8.1 with Update 1: Version 6.3.9600 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.
5.	Install Microsoft .NET Framework 3.5 if the computer does not have this software installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. The Server Manager window appears. Use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.

Table 39: Upgrading Unified Metasys Server with SCT on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
6.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
7.	If you are installing the Metasys Server software on an English language computer, skip to the next step. If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
8.	Install a version of SQL Server Express software on the computer that the *Metasys* system supports.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
9.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
10.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
11.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
12.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.

Table 39: Upgrading Unified Metasys Server with SCT on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
13.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.
14.	Select the appropriate action: • If you have **SCT Release 7.x to 10.x or SCT 11.1 to 13.x**, skip to the next step. • If you have **SCT Release 6.5.x or earlier, or SCT 11.0**, follow the steps to the right to manually record all SCT users.	1. Log in to SCT and open the Security Administrator tool (**Tools > Administrator**). 2. In Security Administrator, record all SCT roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All SCT customized roles and user accounts are lost when you uninstall SCT in the next step. 3. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role.

Table 39: Upgrading Unified Metasys Server with SCT on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
15.	As part of performing an out-of-place upgrade, follow the steps to the right.	1. Disconnect the old ADS/ADX computer from the building network. 2. Connect the new computer to the building network. 3. On the new computer, assign the same computer name and IP address as the old ADS/ADX computer. 4. Install and license SCT 14.0 on the new computer. 5. Install Metasys Database Manager Rel. 11.0 on the new computer. 6. Copy the Metasys database backup files (.bak) from the old computer to the Metasys Database Manager Backup folder of the new computer. 7. Copy the SCT archive backup file (.backup) from the old computer to the new computer. Place the archive here: `C:\ProgramData\Johnson Controls\MetasysIII\DatabaseFiles`. 8. Start SCT on the new computer. With SCT, restore the backup you copied in the previous step. 9. If the new computer name is different from the old computer, open the restored SCT archive, upgrade the archive, then rename the Site Director in the upgraded archive to match the new computer name. 10. Start the Metasys Database Manager in Expert mode and restore each database backup from the SQLData backup folder. 11. If the new computer name is different from the old computer, use the Metasys Database Manager to update the Site Director and device names in the Metasys system databases.
16.	Install the Metasys Server 11.0 software.	See Metasys Server Software.
17.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
18.	Install and license any other Metasys Release 11.0 software at this time, including the Metasys Export Utility.	Refer to their respective installation documents. For licensing, refer to the *Software Manager Help (LIT-12012389)*.

Table 39: Upgrading Unified Metasys Server with SCT on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
19.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
20.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
21.	Start Launcher on the computer, and add a profile for Metasys SCT.	Refer to *Launcher Tool Help (LIT-12011742)*.
22.	Start the Metasys SCT from Launcher on the computer and verify proper operation.	Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
23.	Select the appropriate action: • If you upgraded SCT from **Release 7.x or Release 11.1** to Release 14.0, go on to the next step. • If you upgraded SCT from **Release 6.5.x or earlier, or Release 11.0** to Release 14.0, start SCT. Open the Security Administrator tool (Tools > Administrator). In Security Administrator, recreate all roles, user accounts, and Active Directory user accounts that were present in the old version of SCT (or, create a new limited set of SCT users). If you made screen captures of the SCT roles and users in an earlier step, use these screens as a guide for adding the roles and user accounts to SCT.	Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
24.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.
25.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
26.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.

Table 39: Upgrading Unified Metasys Server with SCT on Desktop OS (Out-of-Place)

Step	Action	Reference or Additional Steps
27.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.
28.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
29.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading Unified Metasys Server and SCT on Server OS

Table 40: Supported Platforms Unified Metasys Server with SCT Server OS

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table to perform an out-of-place upgrade of Metasys Server and SCT software on a computer with a server operating system. These steps presume that the computer currently has no Metasys software installed.

Table 41: Upgrading Unified Metasys Server with SCT on Server OS (Out-of-Place)

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	If you are installing the Metasys Server software on an English language computer, skip to the next step. If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
5.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.

Table 41: Upgrading Unified Metasys Server with SCT on Server OS (Out-of-Place)

Step	Action	Reference or Additional Steps
6.	Install Microsoft .NET Framework 3.5 if the computer does not have this software installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. The Server Manager window appears. Use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
7.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
8.	Install a version of SQL Server Standard or Enterprise software on the computer that the *Metasys* system supports. Install these components: Database Engine Services, Reporting Services, and Management Tools.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
9.	Verify that Reporting Services on the computer is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
10.	Install support files on the computer if you plan to offer the Site Management Portal in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
11.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
12.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.

Table 41: Upgrading Unified Metasys Server with SCT on Server OS (Out-of-Place)

Step	Action	Reference or Additional Steps
13.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
14.	Perform a complete backup of **all** historical data in the ADS/ADX computer with the Metasys Database Manager. If the system to be upgraded is at Release 8.0 or 8.1, after the historical databases are backed up, use the SQL Server Management Studio to backup the SpacesAuthorization database.	Refer to *Backing Up a Database* in *Metasys Database Manager Help (LIT-12011202)*.
15.	Make a copy of each historical database backup file and archive backup file and store them on removable media (for example, a flash drive or DVD).	Use Windows Explorer to prepare and archive the file copies.
16.	Select the appropriate action: • If you have **SCT Release 7.x to 10.x or SCT 11.1 to 13.x**, skip to the next step. • If you have **SCT Release 6.5.x or earlier, or SCT 11.0**, follow the steps to the right to manually record all SCT users.	1. Log in to SCT and open the Security Administrator tool (**Tools > Administrator**). 2. In Security Administrator, record all SCT roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All SCT customized roles and user accounts are lost when you uninstall SCT in the next step. 3. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role.

Table 41: Upgrading Unified Metasys Server with SCT on Server OS (Out-of-Place)

Step	Action	Reference or Additional Steps
17.	As part of performing an out-of-place upgrade, follow the steps to the right.	1. Disconnect the old ADS/ADX computer from the building network. 2. Connect the new computer to the building network. 3. On the new computer, assign the same computer name and IP address as the old ADS/ADX computer. 4. Install and license SCT 14.0 on the new computer. 5. Install Metasys Database Manager Rel. 11.0 on the new computer. 6. Copy the Metasys database backup files (.bak) from the old computer to the Metasys Database Manager Backup folder of the new computer. 7. Copy the SCT archive backup file (.backup) from the old computer to the new computer. Place the archive here: `C:\ProgramData\Johnson Controls \MetasysIII\DatabaseFiles`. 8. Start SCT on the new computer. With SCT, restore the backup you copied in the previous step. 9. If the new computer name is different from the old computer, open the restored SCT archive, upgrade the archive, then rename the Site Director in the upgraded archive to match the new computer name. 10. Start the Metasys Database Manager in Expert mode and restore each database backup from the SQLData backup folder. 11. If the new computer name is different from the old computer, use the Metasys Database Manager to update the Site Director and device names in the Metasys system databases.
18.	Install the Metasys Server 11.0 software.	See Metasys Server Software.
19.	License the ADS/ADX software with the Software Manager.	Refer to the *Software Manager Help (LIT-12012389)*.
20.	Install and license any other Metasys Release 11.0 software at this time, including the Metasys Export Utility and Energy Essentials.	Refer to their respective installation documents. For licensing, refer to the *Software Manager Help (LIT-12012389)*.

Table 41: Upgrading Unified Metasys Server with SCT on Server OS (Out-of-Place)

Step	Action	Reference or Additional Steps
21.	Start Launcher on the computer and launch the Site Management Portal (SMP) for the upgraded ADS/ADX.	Refer to *Launcher Tool Help (LIT-12011742)*.
22.	To verify ADS/ADX operation, log in to the ADS/ADX using the MetasysSysAgent user and password.	See Launching the User Interfaces.
23.	Start Launcher on the computer, and add a profile for Metasys SCT.	Refer to *Launcher Tool Help (LIT-12011742)*.
24.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.
25.	Select the appropriate action: • If you upgraded SCT from **Release 7.x or Release 11.1** to Release 14.0, go on to the next step. • If you upgraded SCT from **Release 6.5.x or earlier, or Release 11.0** to Release 14.0, start SCT. Open the Security Administrator tool (Tools > Administrator). In Security Administrator, recreate all roles, user accounts, and Active Directory user accounts that were present in the old version of SCT (or, create a new limited set of SCT users). If you made screen captures of the SCT roles and users in an earlier step, use these screens as a guide for adding the roles and user accounts to SCT.	Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
26.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
27.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.

Table 41: Upgrading Unified Metasys Server with SCT on Server OS (Out-of-Place)

Step	Action	Reference or Additional Steps
28.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.
29.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine, downloading the Site Director first (if a network engine is used as the Site Director). The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engine (for example, NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
30.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

Upgrading a Split Metasys Server and SCT

Upgrading a split Metasys system with SCT involves three computers:

- SCT Computer
- Database Server
- Web/Application Server

SCT Computer

Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)* for more information on supported platforms and for installing SCT.

Use the steps in the following table for upgrading SCT on a split Metasys system.

Table 42: Upgrading SCT on Different Computer from Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
1.	Upload and back up all ADS/ADX and network engine archive databases to the existing SCT. Make sure you select the **Include Security** option for the upload.	Refer to *Database Uploading, Downloading, and Synchronization* of *Metasys SCT Help (LIT-12011964)* or the *SCT Technical Bulletin (LIT-1201534)* for the release you have **currently** installed (not the new release).
2.	Forward all trend samples from each network engine to the ADS/ADX Site Director by using the Route Samples command at each engine. This step ensures that the Site Director has all possible samples before you begin the upgrade. Wait a few minutes to ensure that all samples have been forwarded.	Refer to *Metasys Site Management Portal Help (LIT-1201793)* for information about the Route Samples command.
3.	Stop the Metasys III Device Manager service on the ADS/ADX computer. This action prevents the collection of any new audits, alarms, trends, and annotations while you perform the upgrade. If the customer can accept the loss of data samples during an upgrade, you can skip to the next step.	Right-click the Windows taskbar and start Task Manager. Click the **Services** tab. Locate a service called Metasys III Device Manager. Select this service and right-click and select **Stop Service**. The Metasys III Device Manager service stops.
4.	Create a full disk image backup of the computer's hard drive to external media before upgrading any Metasys software (optional but recommended).	Refer to the documentation that came with your operating system backup software.
5.	Uninstall the current version of *Metasys* Launcher from the SCT computer and all clients that log in to the ADS/ADX.	In Control Panel, click **Programs** > **Programs and Features**. Select **Johnson Controls - Launcher** from the list of programs and click **Uninstall**.
6.	Select the appropriate action: • If the site is at Release 7.0 or earlier, uninstall the NAE Update Tool if present. This uninstall step is required before you can install or upgrade to the new version of SCT. • If the site is at Release 8.0 or later, skip to the next step.	In Control Panel, click **Programs** > **Programs and Features**. Select the program from the list and click **Uninstall**.

Table 42: Upgrading SCT on Different Computer from Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
7.	Select the appropriate action: • If you have **SCT Release 7.x to 10.x or SCT 11.1 to 13.x**, skip to the next step. • If you have **SCT Release 6.5.x or earlier, or SCT 11.0**, follow the steps to the right to manually record all SCT users.	1. Log in to SCT and open the Security Administrator tool (**Tools > Administrator**). 2. In Security Administrator, record all SCT roles, local user accounts, and Active Directory user accounts that you want to recreate in the upgraded SCT. All SCT customized roles and user accounts are lost when you uninstall SCT in the next step. 3. For easy recall later, you may find it helpful to use the computer's print screen function to capture the user access permissions and other information for each role.
8.	Select the appropriate action: • If you have **SCT Release 6.5.x or earlier**, skip to the next step. • If you have **SCT Release 7.0 to 13.1**, follow the steps to the right. • If you have **SCT Release 13.2 or 13.3**, upgrade to SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.	1. Uninstall the existing SCT 7.0 to SCT 13.1 software. To retain the SCT security database, make sure that you **uncheck** the box for removing databases. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install SCT 14.0 software. Then license the SCT 14.0 software with the Software Manager. For details, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
9.	Select the appropriate action: • If you have **SCT Release 7.0 or later**, skip to the next step. • If you have **SCT Release 6.5.x or earlier**, follow the steps to the right.	1. Uninstall the existing SCT 6.5.x or earlier software. The SCT and ADS/ADX security databases are not separate at Release 6.5.x or earlier, so an SCT upgrade option is not available. Refer to the *Uninstalling SCT* section of the *SCT Installation and Upgrade Instructions (LIT-12012067)*. 2. Install and license the SCT 14.0 software. Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
10.	Start SCT from the Launcher or the Metasys SCT shortcut. Log in with the MetasysSysAgent user and password. The login process could take a little longer than usual.	Refer to *Launcher Tool Help (LIT-12011742)*.

Table 42: Upgrading SCT on Different Computer from Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
11.	Select the appropriate action: • If you upgraded SCT from **Release 7.x or Release 11.1** to Release 14.0, go on to the next step. • If you upgraded SCT from **Release 6.5.x or earlier, or Release 11.0** to Release 14.0, start SCT. Open the Security Administrator tool (Tools > Administrator). In Security Administrator, recreate all roles, user accounts, and Active Directory user accounts that were present in the old version of SCT (or, create a new limited set of SCT users). If you made screen captures of the SCT roles and users in an earlier step, use these screens as a guide for adding the roles and user accounts to SCT.	Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
12.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.
13.	Go to the next section to upgrade the database server of the split ADX.	Go to Database Server.

Database Server

Table 43: Supported Platforms Split Metasys Server for Database Server

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Use the steps in the following table for upgrading the database component of the ADX on a split Metasys system.

Table 44: Upgrading Database Server on Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
3.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.
4.	Install Microsoft .NET Framework 3.5 if the computer does not have this software installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. The Server Manager window appears. Use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.
5.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
6.	If you are installing the Metasys Server software on an English language computer, skip to the next step. If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
7.	Install a version of SQL Server Standard or Enterprise software on the computer that the Metasys system supports. Make sure you include the Database component, but you do not need to also include the Reporting Services component.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240).*

Table 44: Upgrading Database Server on Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
8.	As part of performing an out-of-place upgrade, disconnect the old database computer and web/application computer from the building network, then connect the new database computer and web/application computer to the building network. Then, follow the steps to the right.	1. On the new database computer and web/application computer, assign the same computer name (**case sensitive**). Use the same IP address information as the old database computer and web/application computer. 2. Install the Metasys Database Manager on the new database computer. 3. Copy the Metasys database backup files (.bak) from the SCT computer that you created in the previous section to the Metasys Database Manager Backup folder of the new database computer. 4. On new database computer, start Metasys Database Manager in Expert mode; restore each database backup file (.bak) from the SQLData backup folder. 5. If the new Application/Web Server name matches the old database name, go to the next step. If the new Application/Web Server name is different from the old database name, click the **Rename** tab in the *Metasys* Database Manager and replace the old Site Director name with the new Site Director name for all device references. Follow the steps in the *Renaming Field Contents in Metasys Databases* section of *Metasys Database Manager Help (LIT-12011202)*. 6. Using Launcher, start SCT on the SCT computer. Open the archive database by clicking Item > Open Archive. If the old archive is missing, restore the database with Tools > Database > Restore Backup. 7. Open the archive with Item > Open Archive. Click **Upgrade**. 8. If the new Application/Web Server name matches the old database name, go to the next step. If the new name is different from the old Application/Web Server name, rename the Site Director in the upgraded archive to match the new computer name.

Table 44: Upgrading Database Server on Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
9.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
10.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.
11.	Go to the next section to upgrade the web/ application server of the split ADX.	Go to Web/Application Server.

Web/Application Server

Table 45: Supported Platforms Split Metasys Server for Web/Application Server

Supported Operating System	Supported Database Options
Windows® Server® 2019 (version 1803 or later) (64-bit) Windows® Server® 2016 with Update (KB4512495) (64-bit)	SQL Server® 2019 (64-bit) SQL Server® 2017 with CU17 (64-bit) SQL Server® 2016 with SP2 CU10 (64-bit) SQL Server® 2014 with SP3 CU4 (64-bit)

Follow these steps to upgrade the web/application component of the ADX on a split Metasys system.

Table 46: Upgrading Web/Application Server on Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
1.	Verify that the computer intended for Metasys Server software is running one of the following supported Windows Server operating systems: • Windows® Server® 2019 (version 1803 or later) (64-bit) • Windows® Server® 2016 with Update (KB4512495) (64-bit) Also run Windows Update to verify the operating system is up to date.	Open a command prompt window and run the command **msinfo32**. Verify the version against the following list: • Windows Server 2019: Version 10.0.118362 • Windows Server 2016: Version 10.0.14393 Start **Windows Update** from the Search box and apply all required and recommended updates before installing any Metasys software.
2.	Verify that the computer name is valid for Metasys Server software.	In Control Panel, click **System and Security > System** and verify the computer name that appears in the window meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A-Z (upper or lower case), numbers 0-9, and hyphens ⓘ **Note:** Underscores are not valid for the Metasys system. • does not end in letters ADS • does not contain any diacritic or accent marks
3.	Configure the Windows Firewall to ensure the ports that Metasys software requires are open.	See Configuring the Windows firewall.
4.	If the computer has multiple network cards, configure the network card that the Metasys Server software is to use.	See Configuring Additional Network Cards.
5.	Install Microsoft .NET Framework 3.5 if the computer does not have this software installed.	In Control Panel, click **Programs** > **Programs and Features** > **Turn Windows features on and off**. The Server Manager window appears. Use the Add Roles and Features Wizard in Server Manager to add the .NET Framework 3.5 Features and HTTP Activation components. On some server-class OSs, HTTP Activation may be listed under WCF Services.

Table 46: Upgrading Web/Application Server on Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
6.	Make sure all required software components are enabled. The Metasys Server installer does **not** enable all required Windows components. If any required component is missing, server installation and operation can fail.	See Required Windows operating system roles and features for more information.
7.	If you are installing the Metasys Server software on an English language computer, skip to the next step. If you are installing the Metasys Server software on a non-English language computer, you need to set the computer's regional settings and the default language used by the SQL Server database to the same locale as the site default language.	Consult the Microsoft documentation and see Installing Metasys Server for a Non-English Locale.
8.	Install a version of SQL Server software on the computer that the Metasys system supports. Make sure you also include the Reporting Services component if you plan to install the Metasys Advanced Reporting System.	Refer to *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
9.	Verify that Reporting Services on the computer is configured properly.	Refer to the *Verifying SQL Server Reporting Services Configuration* section of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
10.	Install support files on the computer if you plan to offer the Site Management Portal in languages other than English.	Refer to the *Appendix: Reporting Services Language Support for Metasys Advanced Reporting System* of *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.
11.	If you uninstalled ADS/ADX software in a previous step because the site was at Release 7.x or earlier, install the Metasys Server 11.0 software. Otherwise, upgrade the Metasys Server 11.0 software. When you install or upgrade, specify the SCT archive database in the SCT Archive Db field on the Reporting tab screen of the Metasys Server 10.1 installer. Make sure you install the new Metasys Server 11.0 software on the Site Director first. If you have other ADSs/ADXs, upgrade them after the Site Director.	See Upgrading Metasys Server or Metasys Server Software.
12.	License the ADS/ADX software with the Software Manager.	License the ADS/ADX software with the Software Manager.
13.	Log in to SCT 14.0 and open the archive database. Allow SCT to upgrade the database to Release 14.0.	Refer to *Metasys SCT Help (LIT-12011964)*.

Table 46: Upgrading Web/Application Server on Split Metasys Server (Out-of-Place)

Step	Action	Reference or Additional Steps
14.	Download the Site Director archive database from SCT 14.0 to the ADS/ADX Site Director, making sure that you click **Include Security**. When asked to enter the ADS/ADX user credentials, specify the MetasysSysAgent user and password. If the login for the ADS/ADX fails, click the **Clear Security Database** tab and click **Set to be cleared**. The device is upgraded, but the security database is removed from the archive.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
15.	If the site has other ADS/ADX servers, upgrade and download each ADS/ADX archive database from SCT 14.0 to the other ADS/ADX servers. The download also restores user accounts.	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
16.	Update the network engines that you want to upgrade to Release 11.0. ⓘ **Note:** If you are upgrading from Release 5.2 or later, you do not need to update all devices to the newer release (except the Site Director). SCT 14.0 supports devices at multiple Metasys software releases, beginning with Release 5.2.	Refer to *NAE Update Tool Help (LIT-12011524)* and *Metasys SCT Help (LIT-12011964)*.
17.	If you updated network engines to Release 11.0, use SCT 14.0 to download the archive database of each network engine. The download also restores the Security database. After the download completes, issue the **Reset Device** command to each downloaded N40-class device (NxE35, NIE39, NxE45, NIE49, NxE25, or NIE29s) to ensure that the security database is archived to non-volatile memory. This step is new beginning at Release 8.0, but **is not** required for any other network engines (NxE55s, NxE59s, SNEs, and SNCs).	Refer to *Database Uploading, Downloading, and Synchronization* in *Metasys SCT Help (LIT-12011964)* for information on downloading.
18.	(OPTIONAL) If you want to move the Metasys historical databases now, use SQL Management Studio to move the databases to the desired location.	See Moving Metasys Historical Databases to a Custom Location.
19.	(OPTIONAL) If you need the server to be FIPS compliant, enable FIPS mode and install the Metasys FIPS component.	See Enabling and installing FIPS component.
20.	Create a full disk image backup of the computer's hard drive to external media (optional but recommended).	Refer to the documentation that came with your operating system backup software.

SQL Server Software

➧ **Important:** See *Appendix: Special Features* if you are installing a split ADX or an ADX with the Metasys Advanced Reporting System. The *Appendix: Special Features* section contains information you should know **before** you follow the steps in this section.

Before you install or upgrade your SQL Server software, consider the following information:

- Microsoft SQL Server 2012, SQL Server 2008, and SQL Server 2008 R2 are no longer supported. For information about how to upgrade SQL Server, refer to *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
- If your computer has SQL Server software installed, verify that its version is supported for the current version of Metasys software. Go to Verifying your computer has a supported version of SQL Server software installed.
- A tool called the SQL Installer is provided on the License Portal with the Branch Tools download to help you **install** or **upgrade** to any supported version of SQL Server software. If you do not have this tool, refer to the *SQL Server Software Installation and Upgrade Instructions (LIT-12012240)* for details on how to install or upgrade SQL Server software. Also refer to *SQL Server Software Installation and Upgrade Instructions (LIT-12012240)* this document if you need to apply a new service pack (SP) to an existing installation of SQL Server software because the SQL Installer does not support service pack installations.
- To use the SQL Installer to install a full version of SQL Server software (for example, SQL Server 2017 Standard edition), you need the Microsoft SQL Server media. To use SQL Installer to install an Express version of SQL Server software (for example, SQL Server 2017 Express), download the SQL Server Express installation file from the Microsoft SQL Server Express website.
- The SQL Installer supports both unified ADS/ADX and split ADX installations, with or without the Metasys Advanced Reporting Services, as well as any SCT configuration. However, the SQL Installer does **not** support adding Reporting Services because these newer versions of SQL Server use a standalone Reporting Services installer. If you have a split ADX with the Metasys Advanced Reporting System, you install the Database Engine Services component of SQL Server on the database server and the Reporting Services component on the web/application server. If you have a split ADX without Metasys Advanced Reporting Services, you only need to install SQL Server on the database server.
- The SQL Installer verifies that your computer has the prerequisites you need to install SQL Server. For example, SQL Server 2014 requires Microsoft .NET Framework version 3.5, but newer versions require Microsoft .NET Framework 4.7.2. An error message appears if a prerequisite is not present. You need to install any missing software prerequisites before continuing.
- The SQL Installer provides an advanced mode that lets you edit the SQL Server command line options before you start the installation. You can also copy the options, paste them into a command window, and run the installation at a command prompt. However, use this method only if you are an advanced user who fully understands SQL Server software options.
- If you are installing SQL Server software manually, we recommend that you **do not** enable the C2 audit tracing feature. With C2 audit tracing enabled, SQL Server creates a large number of operational log files that might eventually fill the hard disk and crash the server. However, if you install MVE, the MVE installer **enables** the C2 audit tracing feature for you. If you want to conserve hard disk space, be sure to disable C2 audit tracing after installing MVE.

- At Release 11.0, the Metasys Advanced Reporting System and Energy Essentials are compatible with SQL Server 2017, SQL Server 2016, and SQL Server 2014 software, but are **not** compatible with SQL Server 2019.
- The SA password that you specify in the SQL Installer window must follow the rules for Microsoft complex passwords. For more information about complex passwords, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
- As part of the installation, the SQL Installer may require you to select an instance name. If you are installing a **unified** ADS/ADX, a stand-alone SCT computer, or the database server of a split ADX, we recommend that you use the default instance name. If you are installing the web/ application server of a **split** ADX, use the instance name of MSSQLSERVER. This requirement is because the ADX install and rename processes assume an instance name of MSSQLSERVER on the web/application server that runs the Reporting Services feature of SQL Server.
- SQL Server installation packages no longer include Management Tools after SQL Server 2016. If you use this server, or a later version, you must manually install the SQL Server Management Studio tool. For details on how to install SQL Server Management Studio after you install SQL Server software, refer to the *SQL Server Software Installation and Upgrade Instructions (LIT-12012240)*.
- If you are installing Metasys server software on a server class machine, SQL Server software must be installed and running **before** you install Metasys software. For a split ADX, the SQL Server software on the database server and SCT computer must be running.
- If after you upgrade to a newer version of SQL Server software, you need to open the Metasys archive database in an older version of SQL Server software, use the Export Database option in SCT. Then import the archive that uses an older version of SQL Server software into SCT.

If your computer has SQL Server software installed, go to Verifying your computer has a supported version of SQL Server software installed to verify that you have a version the Metasys software supports.

Table 47: SQL Server Configuration Selections

SQL Server Configuration Screen	SQL Server Express Edition Selections	SQL Server Standard or Enterprise Edition Selections
Setup Role	N/A	**SQL Server Feature Installation**
Feature Selection	**Database Engine Services** **Management Tools - Basic** (if available)	**Unified ADX/ODS or SCT:** Database Engine Services Reporting Services Management Tools - Basic Management Tools - Complete **Database server on split ADX:** Database Engine Services Management Tools - Basic Management Tools - Complete **Web/application server on split ADX:** Reporting Services Management Tools - Basic Management Tools - Complete
Instance Configuration	**Default Instance** (Named instance is valid as well)	**Default Instance** (Named instance is valid as well) ⓘ **Note:** For a split ADX that will not be renamed in the future, use the default instance for the SQL service on the web/application server and a named instance for the SQL service on the database server. Also, if two web/application servers point to one database server, point each web/application server to a unique SQL Server instance on the data server.

Table 47: SQL Server Configuration Selections

SQL Server Configuration Screen	SQL Server Express Edition Selections	SQL Server Standard or Enterprise Edition Selections
Server Configuration	**SQL Server Database Engine:** NT Service\SQLSERVERAGENT or NT AUTHORITY\SYSTEM **SQL Server Browser:** NT AUTHORITY\LOCAL SERVICE	**SQL Server Agent:** NT Service\SQLSERVERAGENT or NT AUTHORITY\SYSTEM **SQL Server Database Engine:** NT Service\SQLSERVERAGENT or NT AUTHORITY\SYSTEM **SQL Server Reporting Services:** NT Service\SQLSERVERAGENT or NT AUTHORITY\SYSTEM **SQL Server Browser:** NT AUTHORITY\LOCAL SERVICE
Database Engine Configuration	**Mixed Mode** **Specify SQL Server Administrators:** BUILTIN\ADMINISTRATORS (Administrators)	**Mixed Mode** **Specify SQL Server Administrators:** BUILTIN\ADMINISTRATORS (Administrators)
Reporting Services Configuration	N/A	**Unified ADX/ODS or SCT:** Reporting Services Native Mode: Install and configure **Web/application server on split ADX:** Install but do not configure the report server.
SQL Server Configuration Manager **Protocols for <instance name>**	**Named Pipes:** Enabled **TCP/IP:** Enabled	**Named Pipes:** Enabled **TCP/IP:** Enabled

Verifying your computer has a supported version of SQL Server software installed

1. Open the SQL Server Configuration Manager tool.

   ⓘ **Note:** If you do not see any version of Microsoft SQL Server on your computer, you do not have the required software. Follow the instructions in this document for installing a supported version of SQL Server software.

2. In the left pane, select **SQL Server Services**. In the right pane, double-click the **SQL Server** instance name.
3. Click the **Advanced** tab and scroll down to the **Version** row.
4. If the version matches any of the listed version numbers, you have a supported version of SQL Server or SQL Server Express software. Verify that the version number is any one of the following or later versions:

   - 15.0.2000.5: SQL Server® 2019 (64-bit)
   - 14.0.3238.1: SQL Server® 2017 with CU17 (64-bit)
   - 13.0.5492.2: SQL Server® 2016 with SP2 CU10 (64-bit)
   - 12.0.6329.1: SQL Server® 2014 with SP3 CU4 (64-bit)

5. If the version **does not** match any of these version numbers or later, you need to either apply the required service pack or upgrade to a newer version of SQL Server or SQL Server Express software. Follow the instructions in the *SQL Server Install and Upgrade Installation Instructions (LIT-12012240)* for installing a supported version of SQL Server software.

Uninstalling MVE Software

About this task:

ⓘ **Note:** If MVE is installed on the computer with ADX software, uninstall MVE before you uninstall ADX. MVE Software

1. In Control Panel, select **Add or Remove Programs**. Select **Programs** > **Programs and Features**.
2. Select **Metasys Validation Environment**.
3. Click **Change/Remove** or **Uninstall**.
4. Click **Uninstall**. A progress screen appears while MVE is removed from the computer.
5. Click **Finish**.
6. Disable C2 audit mode if you had this SQL Server feature enabled for the MVE site. For details, refer to the *Enabling or Disabling C2 Security* section in the *Metasys for Validated Environments Extended Architecture Technical Bulletin (LIT-12011327)*.
7. Uninstall the existing ADX software. Go to Uninstalling the Metasys Server Software Introduction.

Uninstalling the Metasys Server Software

Introduction

- **Important:** If you receive error messages when you uninstall Metasys Server (ADS/ADX) software, you may have problems reinstalling it. Diagnose these problems before you attempt to reinstall the software.

- **Important:** The Metasys Server is offline from when you uninstall the software to when you finish the upgrade or reinstallation. Be aware that if your historical databases are over 500 MB, the upgrade may take several hours to complete. Consider using the Metasys Database Manager or SQL Server software tools to purge your historical database prior to an upgrade. Refer to the *Metasys Database Manager Help (LIT-12011202)* for details.

ⓘ **Note:** The Metasys Server software must be able to communicate with the SQL Server databases during the uninstallation process.

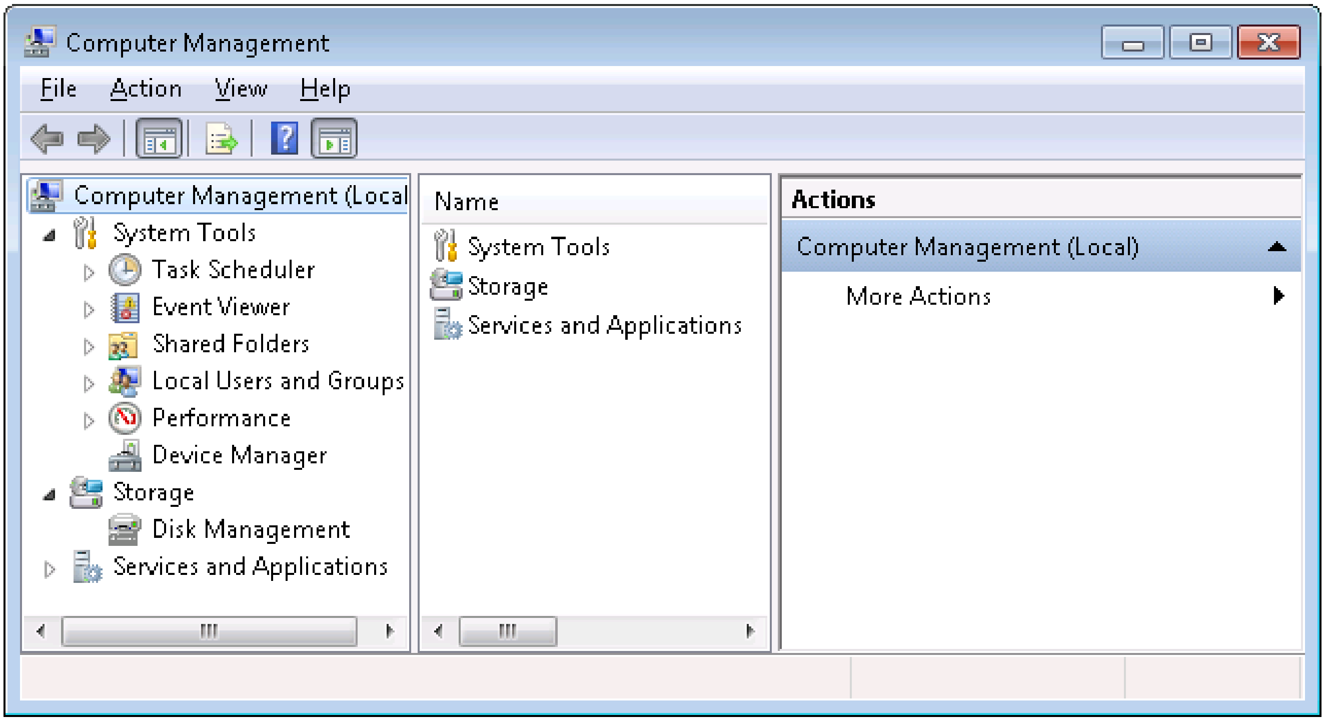
Clearing Out Pending Event Messages from Message Queue

About this task:

ⓘ **Note:** Follow this procedure only if you are upgrading from Metasys system Release 5.0 or later.

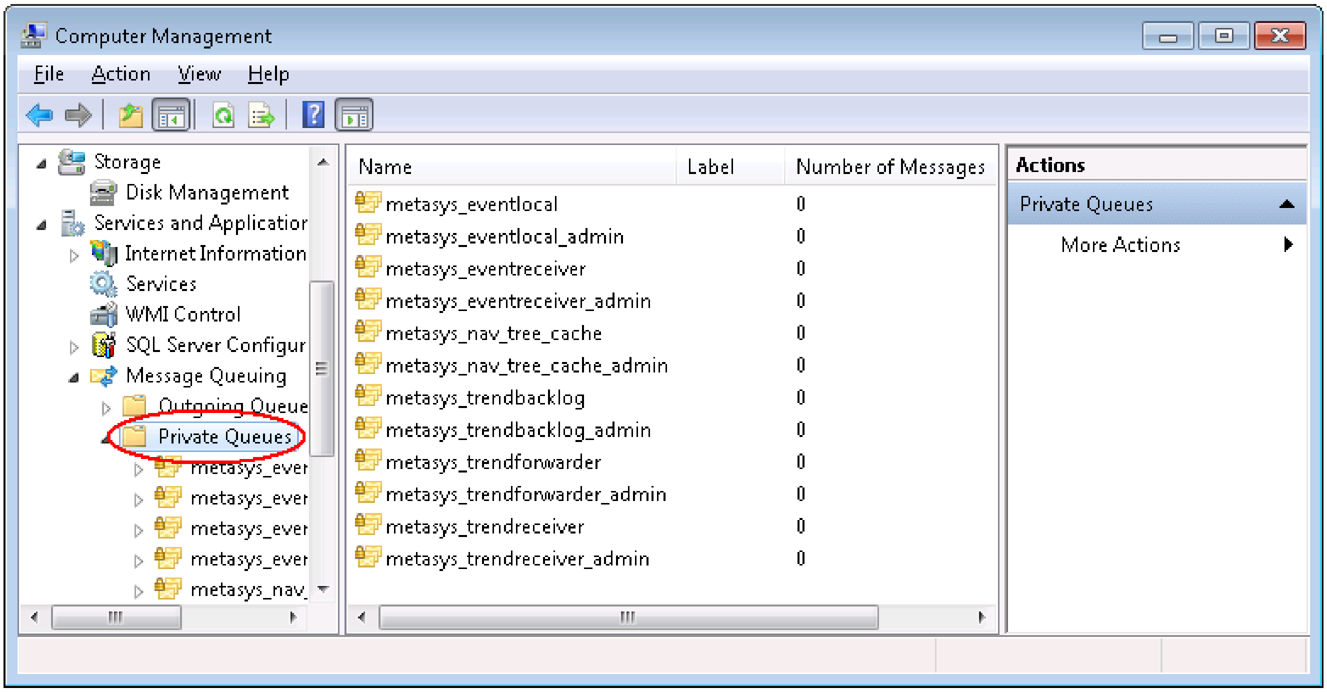
1. Log in to the computer that you intend to upgrade the Metasys Server software.
2. End the Metasys III Device Manager task on the Metasys Server computer. Right-click the **Windows taskbar** and start **Task Manager**. Click the **Processes** tab and click **Show processes for all users**. Locate a task called **Metasys III Device Manager**. Select this task and click **End Task** or **End Process**. The Metasys III Device Manager service stops.
3. On the Start menu, click **Run** or hold down the Windows key and press **R**. The Run box appears.
4. In the Run box, type `compmgmt.msc` and click **OK**. The Computer Management screen appears (Figure 1).

Figure 1: Computer Management Window



5. In the left pane, expand **Services and Applications > Message Queuing > Private Queues**. Select **Private Queues** so that the Metasys queues appear (Figure 2).

Figure 2: Computer Management: *Metasys* Private Queues



Name	Label	Number of Messages
metasys_eventlocal		0
metasys_eventlocal_admin		0
metasys_eventreceiver		0
metasys_eventreceiver_admin		0
metasys_nav_tree_cache		0
metasys_nav_tree_cache_admin		0
metasys_trendbacklog		0
metasys_trendbacklog_admin		0
metasys_trendforwarder		0
metasys_trendforwarder_admin		0
metasys_trendreceiver		0
metasys_trendreceiver_admin		0

6. Verify that the number of messages in each of these Metasys queues is 0:

   metasys_trendreceiver
   metasys_trendforwarder
   metasys_trendbacklog

These are the only queues that may contain customer critical data.

7. If each of these Metasys queues has 0 messages, go to Step 8.

   If any of these Metasys queues has one or more messages, contact the Johnson Controls Field Support Center (FSC) for further instruction. Do not proceed to the Metasys Server uninstall steps until FSC helps you manually process the event messages.

8. Select each Metasys queue under the Private Queues table and select **Action > Delete**. Repeat until you have deleted all Metasys queues. Go to Step 11.

   ⓘ **Notes:**

   - If you do not have operating system permission access to delete the queues, you need to take ownership of each queue. Go to Step 9.
   - If the operating system displays an error message indicating that you cannot take ownership of any queue, go to Step 10.

9. To take ownership of a Metasys queue, right-click the queue and select **Properties**. Select the **Security** tab and then click **Add**. In the Select Users or Groups window, type **Administrators**, and then click **Check Names** to select the Administrators account. Click **OK**. In the queue's Properties dialog box, select **Full Control** under the Allow column. Click **OK** to complete the process. Go back to Step 8 to delete the Metasys queues.
10. Uninstall the Message Queuing component from Windows, making sure that the operating system media is available or that your hard disk contains the files necessary for the reinstallation. The process to uninstall Message Queuing varies slightly depending on your operating system:

    - If you are using Windows 10 or Windows 8.1 in Control Panel, select **Programs > Programs and Features > Turn Windows features on or off**. Clear the Microsoft Message Queuing Server Core component check box, and follow the steps to complete the uninstallation.
    - If you are using Windows Server 2019 or Windows Server 2016, in Control Panel, select **Programs > Programs and Features > Turn Windows features on or off**. The Server Manager Dashboard and the Add Roles and Features Wizard appear. In the Server Manager Dashboard, click **Local Server**, and then click **Manage** > **Remove Roles and Features**. The Remove Roles and Features Wizard appears. Click **Next** until you reach the Remove features screen. Locate Message Queuing in the Features table. Clear the check box for Message Queuing. All related check boxes also clear. Click **Next**, then click **Remove** to proceed with the removal of Message Queuing.

11. Close the Computer Management window.

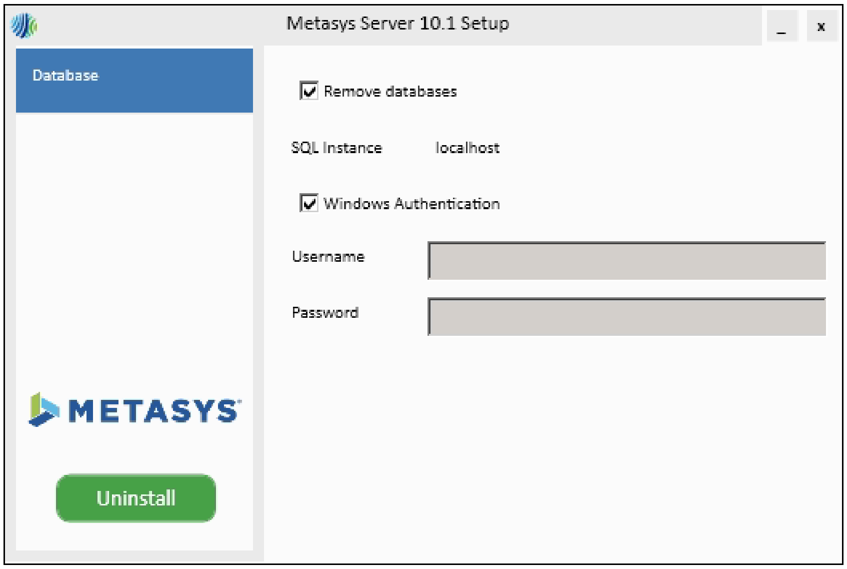
Uninstalling Metasys Server Software

Follow the steps in this section for uninstalling the current version of Metasys Server software from a computer. However, if you have Metasys Server software at Release 8.x or later, and you intend to install Release 11.0, you can skip this section and go directly to Upgrading Metasys Server. The only exception is if you are upgrading to a different software build of the Metasys Server at the same release level (for example, 11.0.0.4570 to 11.0.0.5847). In this case, you must first **uninstall** the ADS/ADX software, then install the newer build.

Note: The Remove databases option on the uninstall screen is selected by default. If you check this box, the XMS database is removed during uninstall process. No other databases except the XMS database are removed. Therefore, to retain this database, **uncheck** that selection before starting the uninstallation.

1. In Control Panel, click **Programs > Programs and Features**. A list of all installed programs appears.
2. Locate and select the installed release of the **Metasys Server** program item.
3. Click **Uninstall**. The removal process begins. It may take a few moments before the first uninstall window appears.

Figure 3: Uninstall Window



Metasys Server 10.1 Setup

☑ Remove databases

SQL Instance localhost

☑ Windows Authentication

Username

Password

   a. **Remove databases**: check if you want to remove the XMS database during the uninstallation. No other databases except the XMS database are removed.
   b. **Windows authentication**: check if you want to use Windows authentication for uninstalling the software; uncheck if you want to use a SQL Server administrator account. Enter a SQL Server username and password.
   c. **Username**: specify the user name of the SQL Server administrator. This field is enabled only if Windows authentication is not checked.
   d. **Password**: specify the password of the SQL Server administrator. This field is enabled only if Windows authentication is not checked.

4. Click **Uninstall**. Seconds later, the progress screen appears. Wait until all steps have finished.
5. After all steps have completed, the complete box appears.

   a. Click **Restart Now**: a restart is needed to make the changes on your computer.
   b. Click **Finish**: a restart is not needed.

Metasys Server Software

➧ **Important:** If the computer has ADS/ADX software at Release 7.x or earlier installed, you are required to **uninstall** the ADS/ADX software before you upgrade to the Metasys Server 11.0. If the ADS/ADX software is at Release 8.0 or later, you can upgrade. During the uninstall process, be sure to retain your historical data and security data. To ensure that no data is lost, make sure that the buffer size of the supervisory engines is large enough to hold archived data while the ADS/ADX is upgraded to the Metasys Server.

ⓘ **Note:** Regardless of the upgrade release, you must uninstall Energy Essentials, Metasys Database Manager, and MVE prior to upgrading the Metasys Server.

You have the choice of two installation methods: default or custom.

Default Method—select this method for installing or upgrading an ADS and accepting all default options. This method installs English only SQL Server Express 2017 CU19 (if needed), Metasys Server (ADS only), Metasys UI, Launcher, Software Manager, and the software components listed in Table 2. Windows credentials are used for SQL database creation and configuration.

Custom Method—select this method for installing an ADS or ADX and you want to customize the installation options. This method installs the Metasys Server software (ADS or ADX), Metasys Advanced Reporting System (ADX only), Metasys UI, Launcher, Software Manager, and the software components listed in Table 2.

Before you begin the installation process, consider the following important factors:

- The Metasys Server 11.0 may coexist on the same computer as SCT 14.0. If your computer has SCT at Release 11.0 or earlier, you must uninstall the older SCT release before installing Metasys Server 11.0. Refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.
- If something goes wrong with installation, a link called **View Install Log** appears that you can click to open a log file with the default html viewer, such as your web browser. For details about how to use the log viewer, see Metasys Server Log.
- The Metasys Server setup requires at least 8 GB of available hard disk space and at least 8 GB of RAM for successful installation and operation of the Metasys Server software and databases. Verify your computer has at least 8 GB hard disk space before you begin the installation.
- As a requirement for installation or upgrade, the Metasys Server setup requires that its executable file (.exe) and its data file (.data) are stored in the same folder location.
- The Metasys Server setup replaces the SSL certificate binding in IIS, if a non-SHA256 SSL certificate is not already bound.
- Metasys Server installation also includes the installation of Metasys UI, an alternative user interface to the Site Management Portal UI. To log on the Metasys UI, use the same credentials as the Site Management Portal. After installation is complete, the Metasys UI software performs a one-time configuration process in the background that can take up to 30 minutes to complete. During this process, the user log on process is delayed or takes longer than usual until the configuration is complete.
- If you are installing the Metasys Server application on a virtual machine (VM), configure the VM to run in static memory mode, not dynamic. Otherwise, operational issues with SQL Server may result. Also, configure the VM to use at least 8 GB of memory.
- Do not install other software applications on the Metasys Server because they may interfere with Metasys Server operation.

- When you install the Metasys Server 11.0, you must upgrade all other ADSs/ADXs on the site to Release 5.2 software or later. This ADS/ADX restriction is a result of enhancements made in Release 5.2 to improve the speed and reliability of message forwarding.
- If in the future you need to uninstall the Metasys Server, the SQL Server Express software that may have been installed for you remains in place. Also, any changes that the Metasys Server setup made, such as enabling Windows components and features, remain in place; they are not rolled back.
- The Metasys Server setup configures IIS to use TLS 1.2 only. Use of TLS 1.2 is required by all Metasys site devices.
- The Metasys Server software installation on a computer with a server operating system provides you the option of installing the Metasys Advanced Reporting System. Advanced Reporting supports installation on a computer with SQL Server 2017, SQL Server 2016, and SQL Server 2014, but **not** with SQL Server 2019. Also, the Energy Essentials add-on for Metasys Advanced Reporting is compatible with SQL Server 2017, SQL Server 2016, and SQL Server 2014. For more information, refer to the *Metasys Advanced Reporting System and Energy Essentials Help (LIT-12011312)*.

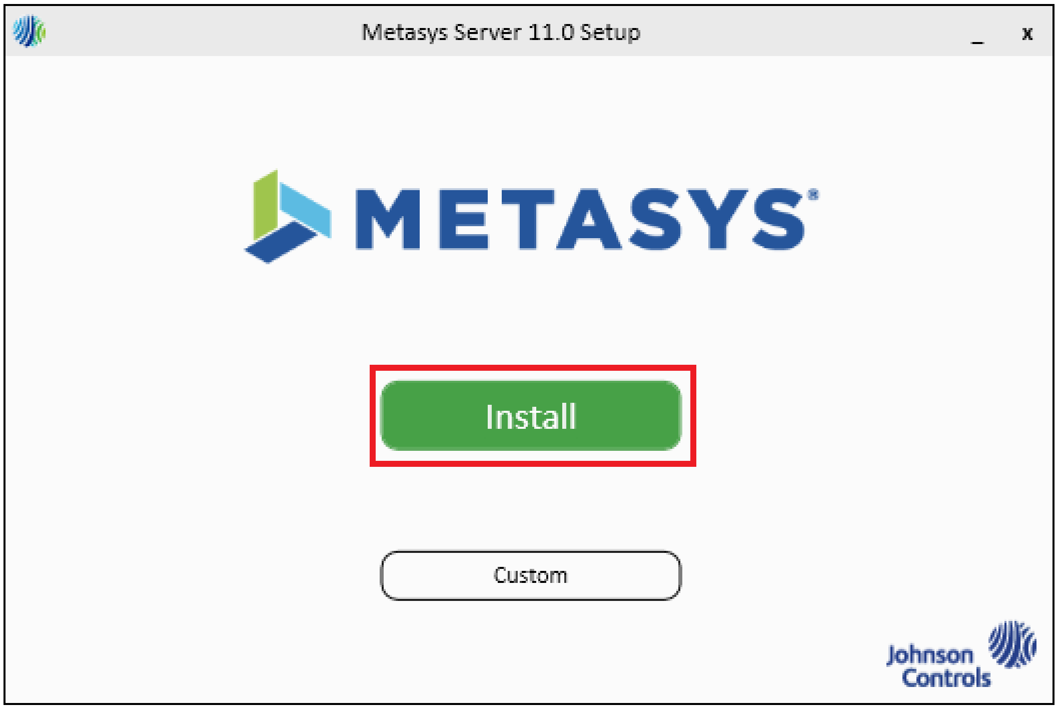
Installing Metasys Server: Default Method

Follow the steps in this section if want to install the Metasys Server software with the default options.

ⓘ **Note:** When you begin the installation process, Metasys Server Setup detects whether the computer has a previous release of ADS/ADX software and meets the prerequisites defined in this document. If pre-Release 8.0 ADS/ADX software is found, a message appears requesting you to **uninstall** the ADS/ADX software first; see Uninstalling Metasys Server Software. If Release 8.0 or later ADS/ADX software is found, an upgrade option is available. Skip this section and go to Upgrading Metasys Server. Also, before you start the installation process, close Software Manager if currently open.

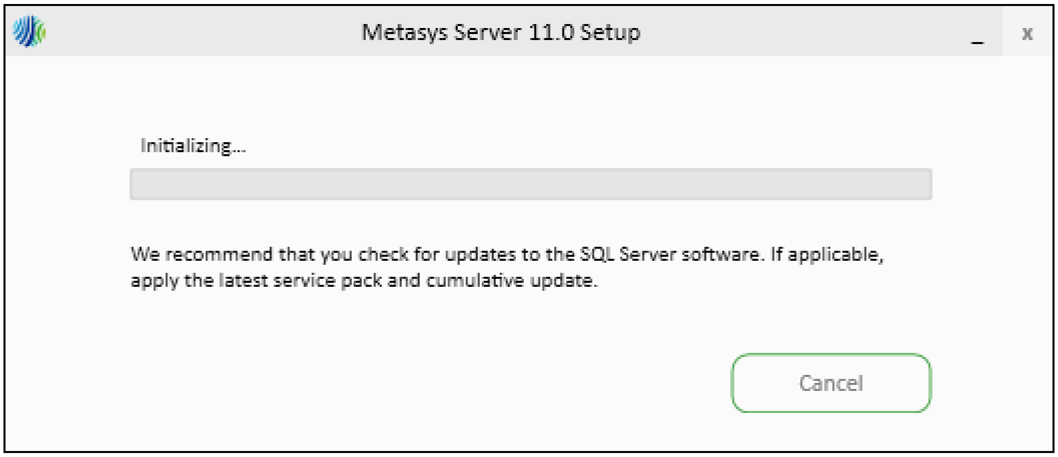
1. Obtain the Metasys Server installation file (MetasysServer_11.0.exe) and Metasys Server data file (MetasysServer_11.0.data). Store both files in the same location.
2. Using Windows Explorer, browse to the location of the Metasys Server installation and data files.
3. Right-click **MetasysServer_11.0.exe** and select Run as Administrator. Enter the Administrator's user credentials if prompted. The setup window appears.

Figure 4: Metasys Server Setup Window



4. Click **Install** on the Metasys Server setup screen. The Initializing screen appears:

Figure 5: Metasys Server Initialization window



Initializing...

We recommend that you check for updates to the SQL Server software. If applicable, apply the latest service pack and cumulative update.

Do **not** click **Cancel**. You can apply any updates after the installer completes. Seconds later, the installer continues and the progress of each step is shown. As part of installation, SQL Server 2017 Express is installed for you if the computer does not have a supported version of SQL Server Express software. Also, if the setup program requires a restart during installation, it prompts you, then resumes installation after the restart.

ⓘ **Note:** If .NET Framework 4.7.2 is missing from the computer, the Metasys Server installation is paused at this point and the .NET Framework 4.7.2 components are installed now, then the computer restarts. After the restart, the Metasys Server installer automatically resumes.

5. After all installation steps have finished, the Metasys Server Setup Complete window appears.

   - Click **Restart Now**: a restart is needed to make the changes on your computer. After the restart, continue with the next step.
   - Click **Finish**: a restart is not needed. Proceed to the next step.

6. If you disabled antivirus software before you began installing the Metasys Server software, after the computer restarts, log in and re-enable the software.
7. (Optional) If the site is trending large amounts of data, resize the MSMQ limitation. For details, refer to *Message Queue Size Considerations* in the *ADS/ADX Commissioning Guide (LIT-1201645)*.
8. License the Metasys Server with the Software Manager, which is installed with the server. For details, refer to *Software Manager Help (LIT-12012389)*.

Installing Metasys Server: Custom Method

Follow the steps in this section if you want to use the custom method of installing Metasys Server software. Use the custom method for any of the following reasons:

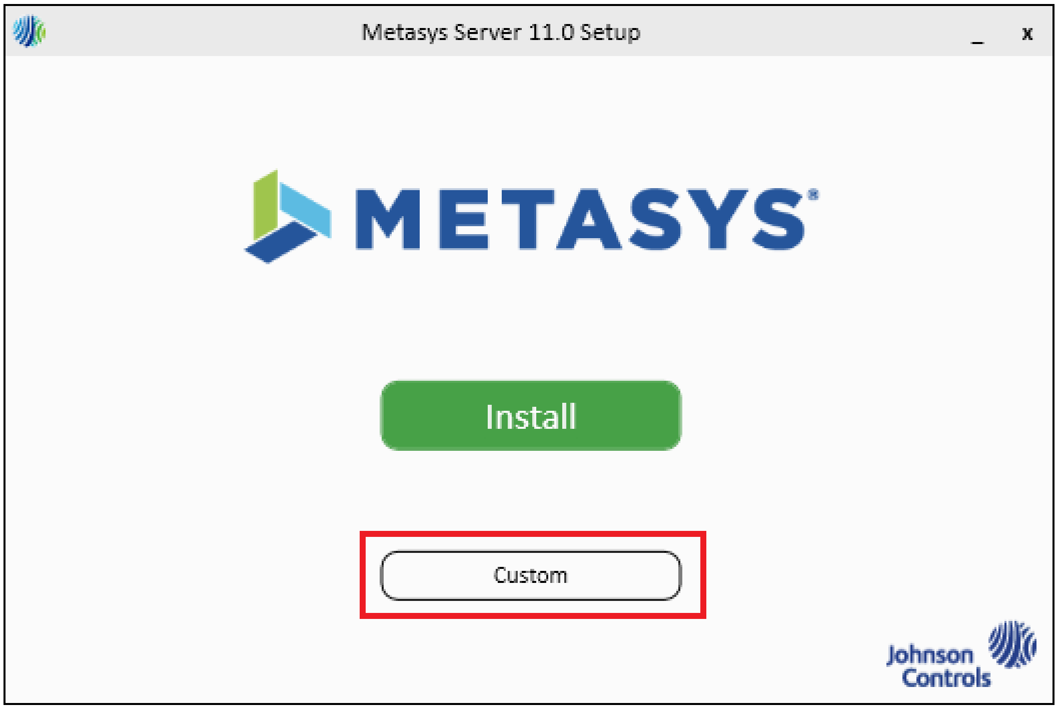
- you want to select a specific SQL Server instance other than MSSQLSERVER
- you want to install the Metasys Server software in a location other than the default location (C:\Program Files (x86)\Johnson Controls)
- you want to install the third-party applications that the Metasys Server uses (RabbitMQ and Erlang/OTP) in a location other than the default location (C:\Program Files (x86)\Johnson Controls)
- you are installing Metasys Server software on a Windows Server operating system
- you want to install the Metasys Advanced Reporting System on the Metasys Server

ⓘ **Note:** If you select the Reporting component in the Metasys Server installation, do not begin the installation process until you have created the database in SCT that you intend to use with the Metasys Advanced Reporting Services. You need to select this database during Metasys Server software installation. Also, verify that this database includes a Site object. Lastly, make sure that Reporting Services is properly configured and running. If you are unsure, refer to the *Verifying SQL Server Reporting Services Configuration* section of the *SQL Server Installation and Upgrade Instructions (LIT-12012240)*.

When you begin the installation process, Metasys Server Setup detects whether the computer has a previous release of ADS/ADX software and meets the prerequisites defined in this document. If pre-Release 8.0 ADS/ADX software is found, a message appears requesting you to **uninstall** the ADS/ADX software first; see Uninstalling Metasys Server Software. If Release 8.0 or later ADS/ADX software is found, an upgrade option is available. Skip this section and go to Upgrading Metasys Server. Also, before you start the installation process, close Software Manager if currently open.

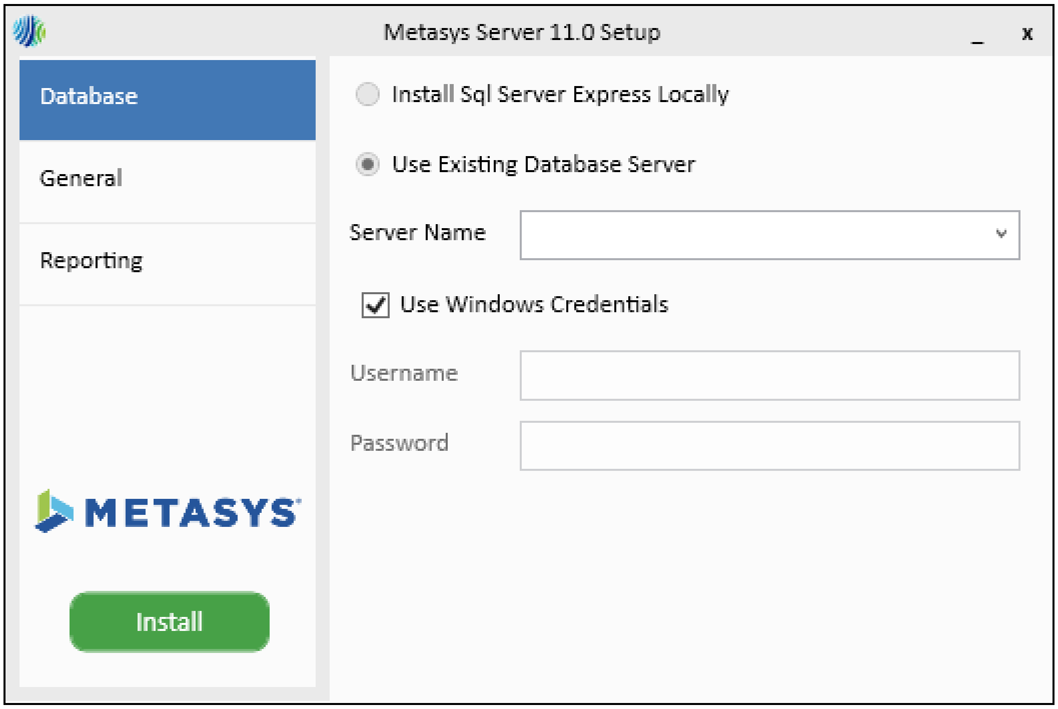
1. Obtain the Metasys Server installation file (MetasysServer_11.0.exe) and Metasys Server data file (MetasysServer_11.0.data). Store both files in the same location.
2. Using Windows Explorer, browse to the location of the Metasys Server installation and data files.
3. Right-click **MetasysServer_11.0.exe** and select Run as Administrator. Enter the Administrator's user credentials if prompted. The setup window appears.

Figure 6: Metasys Server Setup Window



4. Click **Custom**. The Database screen appears.

Figure 7: Metasys Server Database Window



○ Install Sql Server Express Locally

● Use Existing Database Server

Server Name

☑ Use Windows Credentials

Username

Password

5. Under the Database section, select from these options:

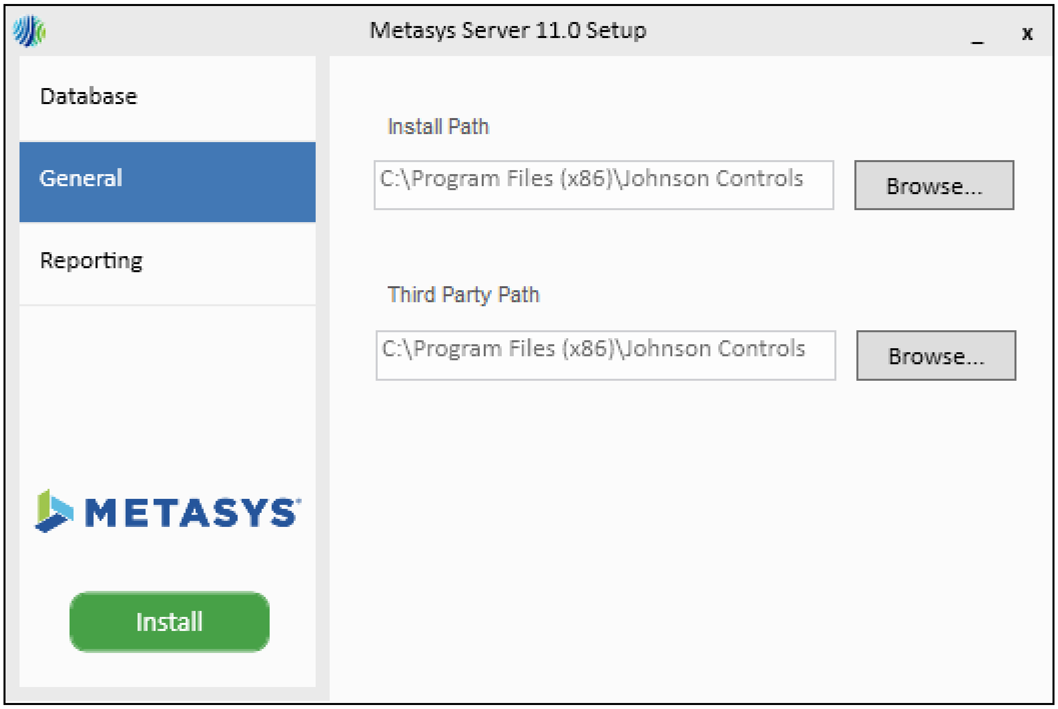
    a. **Install SQL Server Express Locally**: Click this option if you want the Metasys Server Setup program to install a local instance of SQL Server 2017 Express with CU17. This option is disabled on computers with a Windows Server operating system. If the computer has an unsupported version of SQL Server Express software, the installation halts with a message that you must upgrade to a supported version.
    b. **Use Existing Database Server**: Click this option if an instance of SQL Server software is installed on the computer already, then select the server instance name.
    c. **Server Name**: Click the down arrow to select the server name of the SQL database engine installed on the computer. For a unified ADX, you select **(localhost)** in most cases. However, if multiple SQL Server instances are found on the local server, click the one to use for Metasys software. For a split ADX, input the database server name in this format: `<servername>` (default instance) or `<servername>\<database instance>` (named instance).

        ⓘ **Note:** If your installation of SQL Server uses the default instance name, specify only the server name, but do not include the default instance name. Otherwise, an error message appears and you cannot proceed with the installation. You only need to specify a database instance if you have a named instance. Also, if the server name you specify does not resolve, use the server's IP address.

    d. **Use Windows Credentials**: Select if you want the installer to use the Windows OS credentials of the currently logged-in user to access the SQL Server software. The logged-in user **must be** a member of the system administrators (sysadmin) role in SQL Server. After installation, you can remove the SQL Server software system administrator rights from this user if so directed by IT personnel.
    e. **Username** and **Password**: Clear the **Use Windows Credentials** box to enter the SQL Server Administrator login and password credentials in these fields if you want the installer to use a SQL Server login with system administrator rights.

6. Click the **General** tab. The General screen appears.

Figure 8: Metasys Server General Window



Install Path

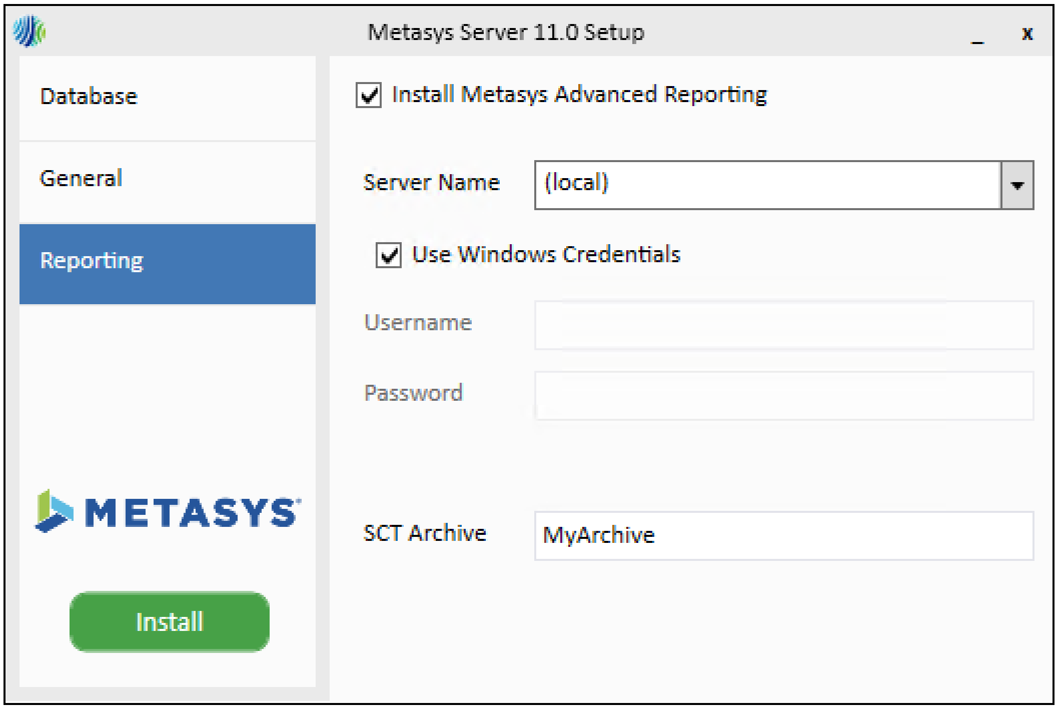
C:\Program Files (x86)\Johnson Controls

Third Party Path

C:\Program Files (x86)\Johnson Controls

7. In the **Install Path** and **Third Party Path** fields, you can either accept the default installation paths or select custom installation locations for the Metasys Server application and third-party applications that the server uses (RabbitMQ and Erlang/OTP). To select a custom location, click **Browse** to select a custom installation location (for example, drive E: instead of drive C:). A Browse For Folder dialog box appears. Select an installation location for each and click **OK**.
8. Click the **Reporting** tab. The Reporting screen appears.

Figure 9: Metasys Server Reporting Window



☑ Install Metasys Advanced Reporting

Server Name: (local)

☑ Use Windows Credentials

Username:

Password:

SCT Archive: MyArchive

9. Under the Reporting section, select from these options:

   a. **Install Metasys Advanced Reporting**: Click to select to install the Metasys Advanced Reporting System. Metasys Advanced Reporting requires a computer with a server operating system that has the Reporting Services component of SQL Server properly configured.

   b. **Server Name**: Specify the computer where the SCT software is installed by either clicking the down arrow or typing the server name. Select the database that SCT uses. Input the server name in this format: **<servername>\<database instance>** (named instance).

      ⓘ **Note:** When you enter the server name of the SCT computer and database instance, do not enter the default instance name. An error message appears and you cannot proceed with the installation. Only enter a database instance if you have a named instance.

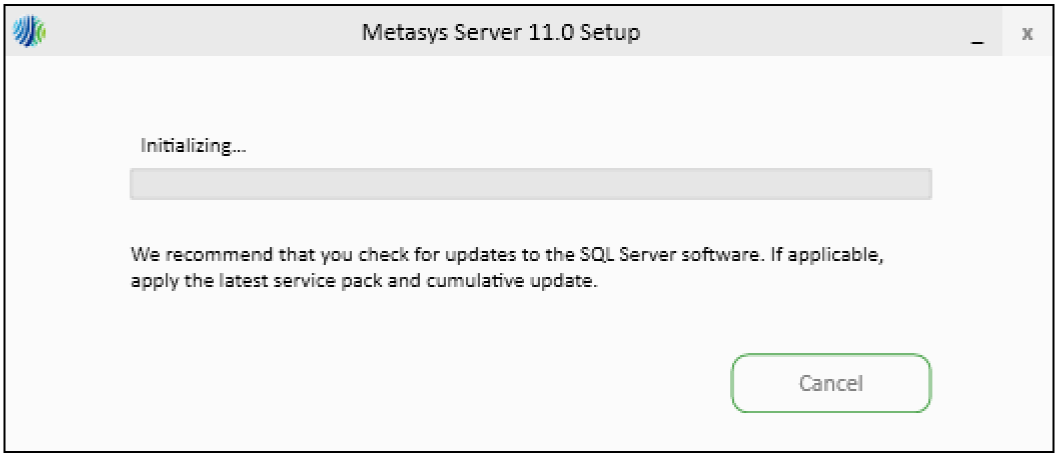
   c. **Use Windows Credentials**: Select if you want the installer to use the Windows OS credentials of the currently logged-in user to access the SQL Server software. The logged-in user **must be** a member of the system administrators (sysadmin) role in SQL Server. After installation, you can remove the SQL Server software system administrator rights from this user if so directed by IT personnel. With SCT installed on a remote computer, the user logged in to the web/application server computer must have system administrator rights to SQL Server.

   d. **Username** and **Password**: Clear the **Use Windows Credentials** box to enter the SQL Server Administrator login and password credentials in these fields if you want the installer to use a SQL Server login with system administrator rights. (If you used the SQL Installer tool to set up SQL Server, you **must** use the SQL Server sa user and password).

   e. **SCT Archive**: Specify the name of the SCT archive that the Metasys Advanced Reporting System is to use. The installer verifies the existence of the archive you specify.

10. To continue, click **Install**. The Initializing screen appears:

Figure 10: Metasys Server Initialization window



Initializing...

We recommend that you check for updates to the SQL Server software. If applicable, apply the latest service pack and cumulative update.

Do **not** click **Cancel**, unless you need to halt installation and apply an update to SQL Server software. Seconds later, the installer continues and the progress of each step is shown.

If the setup program requires a restart during installation, it prompts you, then resumes installation after the restart.

ⓘ **Note:** If .NET Framework 4.7.2 is missing from the computer, the Metasys Server installation is paused at this point and the .NET Framework 4.7.2 components are installed now, then the computer restarts. After the restart, the Metasys Server installer automatically resumes.

11. After all installation steps have finished, the Metasys Server Setup Complete box appears.
    a. Click **Restart Now**: a restart is needed to make the changes on your computer. After the restart, continue with the next step.
    b. Click **Finish**: a restart is not needed. Proceed to the next step.
12. If you disabled antivirus software before you began installing the Metasys Server software, after the computer restarts, log in and re-enable the software.
13. (Optional) If the site is trending large amounts of data, resize the MSMQ limitation. For details, refer to *Message Queue Size Considerations* in the *ADS/ADX Commissioning Guide (LIT-1201645)*.
14. License the Metasys Server with the Software Manager, which is installed with the server. For details, refer to *Software Manager Help (LIT-12012389)*.

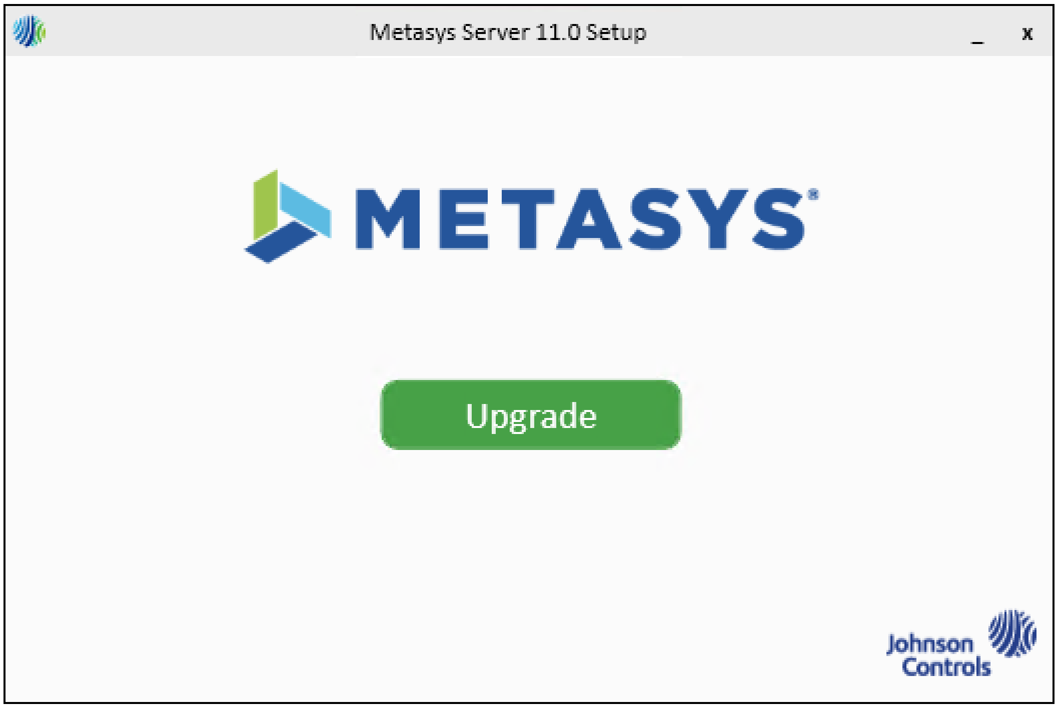
Upgrading Metasys Server

Follow the steps in this section to upgrade the Metasys Server software, an option that is available if you have Release 8.0 or later. If you have Metasys Server software is at Release 7.0 or earlier, go to Uninstalling the Metasys Server Software Introduction. Also, if you have an earlier build of the Metasys Server Release 11.0 software, you cannot upgrade; you must uninstall first, then reinstall. Go to Uninstalling the Metasys Server Software Introduction.

1. Obtain the Metasys Server installation file.
2. Using Windows Explorer, browse to the location of the Metasys Server installation file.

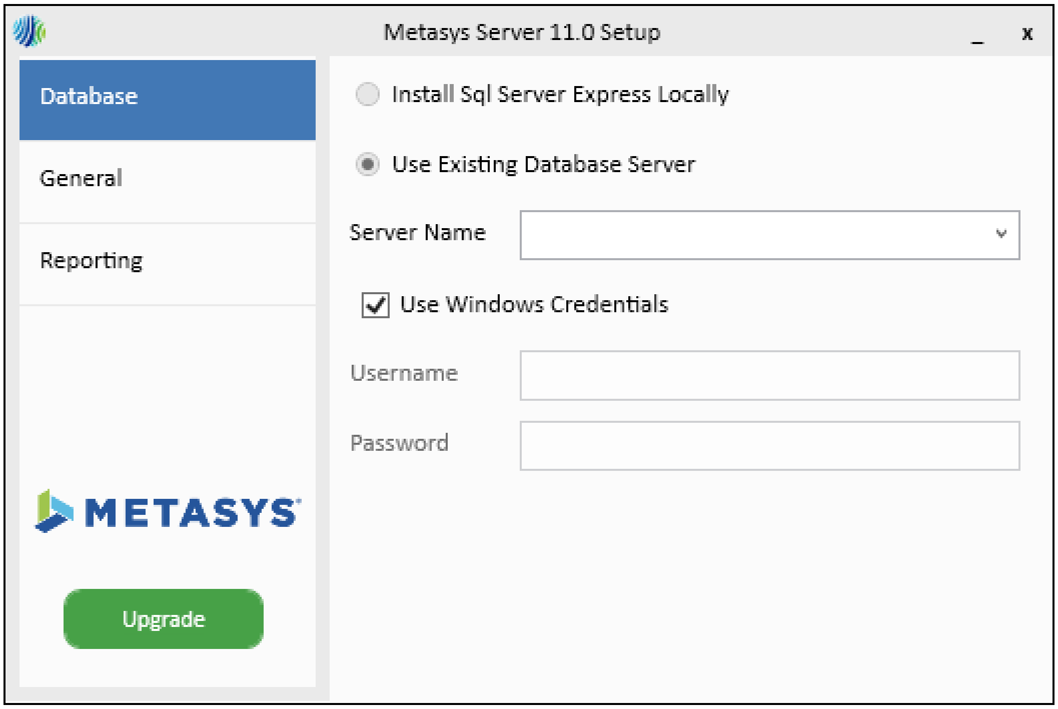
3. Right-click **MetasysServer_11.0.exe** and select Run as Administrator. Enter the Administrator's user credentials if prompted. The setup window appears.

Figure 11: Metasys Server Upgrade Window



4. Click **Upgrade**. The upgrade options screen appears.

Figure 12: Metasys Server Upgrade Options



○ Install Sql Server Express Locally

● Use Existing Database Server

Server Name

☑ Use Windows Credentials

Username

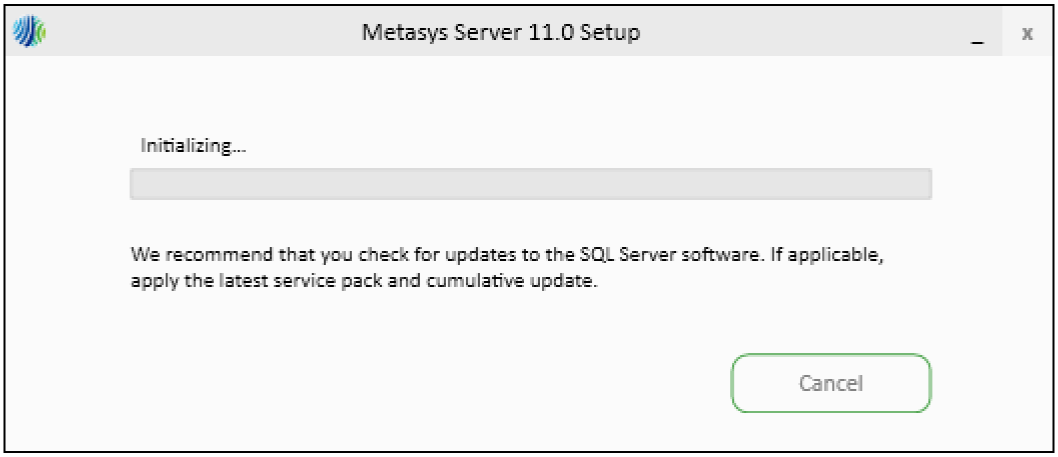
Password

5. Under this setup section, select from these options:

   a. **Server Name**: Verify this read-only field indicates the server name of the SQL database engine installed on the computer (in most cases, localhost).
   b. **Use Windows Credentials**: Select if you want Setup to use the Windows OS credentials of the currently logged-in user to access the SQL Server software. The logged-in user **must be** a member of the system administrators (sysadmin) role in SQL Server. After installation, you can remove the SQL Server software system administrator rights from this user if so directed by IT personnel.
   c. **Username** and **Password**: Clear the **Use Windows Credentials** box to enter the SQL Server Administrator login and password credentials in these fields if you want the setup to use a SQL Server login with system administrator rights.

6. Click **Upgrade**. The setup begins and the Initializing screen appears:

Figure 13: Metasys Server Initialization window



Metasys Server 11.0 Setup

Initializing...

We recommend that you check for updates to the SQL Server software. If applicable, apply the latest service pack and cumulative update.

Do **not** click **Cancel**, unless you need to halt installation and apply an update to SQL Server software. Seconds later, the installer continues and the progress of each step is shown.

The XMS database processing step takes the most time and may show no progress for 15 minutes. This reflects normal operation. Also, for very large databases, this upgrade step may take as long as 30 minutes to complete because of the extensive database refactoring that is required.

ⓘ **Notes:**

- If .NET Framework 4.7.2 is missing from the computer, the Metasys Server upgrade is paused at this point and the .NET Framework 4.7.2 components are installed now, then the computer restarts. After the restart, the Metasys Server upgrade automatically resumes.

- If the user message `If you proceed with the upgrade process, the following Metasys users will be locked out and cannot login: FipsLockUsers.txt` appears during the upgrade process, cancel the upgrade process. Then, for each affected user, set a new password and verify that the Never Expire property under Account Policy is not set. The FipsLockUsers.txt file (located under C:\Users\<user>\AppData\Local\Temp\) lists the user accounts that you need to fix. Additionally, for all other Metasys users, set a new password for any user who has not changed their password in more than two years. Then, restart the upgrade process.
- If the error message `Install complete, but exceptions during historian database upgrade` appears on the Complete screen of the Metasys Server 11.0 software setup, use the Metasys Post Install (MPI) Database tool to complete necessary data type conversion work **before** you restart the computer. For details, refer to the *Database Tools Commissioning Guide (LIT-12012254)*.

7. After all upgrade steps have finished, the Metasys Server Setup Complete box appears.

    - Click **Restart Now**: a restart is needed to make the changes on your computer. After the restart, continue with the next step.
    - Click **Finish**: a restart is not needed, but we recommend that you restart anyway because the licensing service, also updated, often requires a restart. After restarting and logging on the computer, proceed to the next step.

8. If you disabled antivirus software before you began installing the Metasys Server software, after the computer restarts, log in and re-enable the software.
9. (Optional) If the site is trending large amounts of data, resize the MSMQ limitation. For details, refer to *Message Queue Size Considerations* in the *ADS/ADX Commissioning Guide (LIT-1201645)*.
10. License the Metasys Server with the Software Manager, which is installed with the server. For details, refer to *Software Manager Help (LIT-12012389)*.

Licensing the Metasys Server Software

The Metasys Server installation process also installs the Software Manager that you use to license the server and other Metasys applications. For information and instructions on how to properly license the Metasys ADS or Metasys ADX software, refer to the *Software Manager Help (LIT-12012389)*

After you license the Metasys ADS or Metasys ADX software, determine the next step as follows:

- If the customer requires a FIPS compliant system, you must enable FIPS and install FIPS after you license the Metasys Server. Go to Enabling and installing FIPS component.
- If operators at this facility use Graphics+ files, install Microsoft Silverlight 5, a software plug-in that is required to view graphics created with the Graphic Generation Tool. Go to Installing Microsoft Silverlight 5.
- If this facility requires Metasys for Validated Environments software, go to Installing MVE Software.
- If operators at this facility do not use Graphics+ files, the next step is to verify ADS/ADX installation. Go to Launching the User Interfaces.

Enabling and installing FIPS component

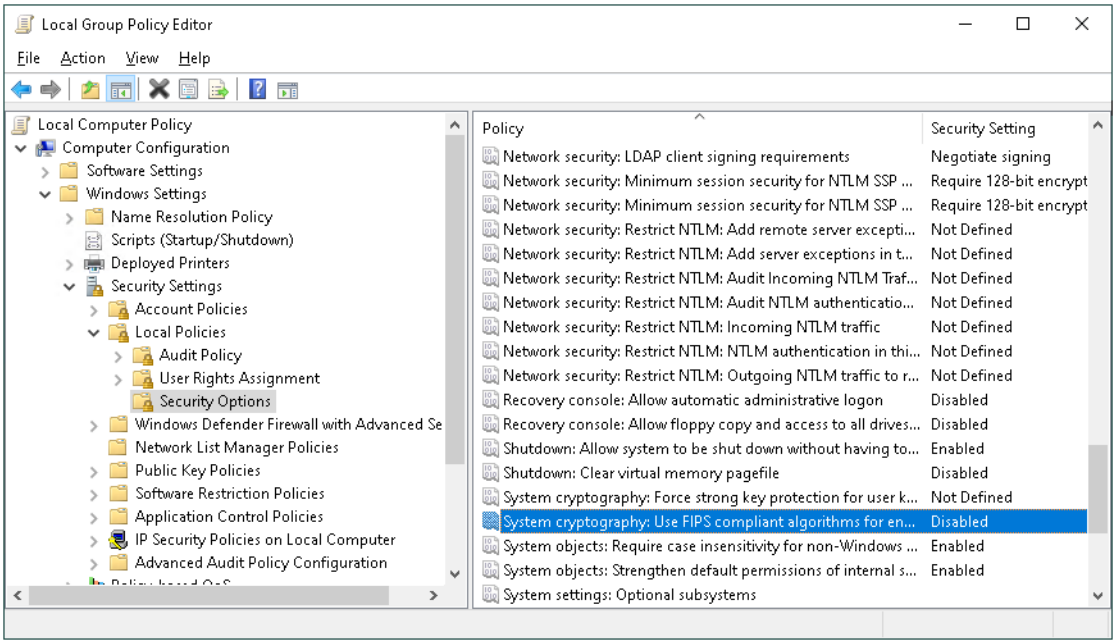
Follow the steps in this section if the customer requires the Metasys Server to comply with the FIPS 140-2 standard. FIPS stands for Federal Information Processing Standard Publication, which defines a set of cryptographic methods used within a government environment. All Microsoft operating systems provide a FIPS mode, but it is disabled by default. Enabling and installing FIPS on the computer that is running the Metasys Server software includes the following steps:

- enabling FIPS on the Windows operating system
- licensing FIPS after the Metasys Server software is installed and licensed
- installing FIPS component for the Metasys Server

Important: If you enable FIPS on your Metasys Server, you must also update all network engines to Release 11.0, because a FIPS-compliant server is restricted from communicating with engines that are non-FIPS compliant. All network engines at Release 11.0 are inherently FIPS compliant, so no additional steps are required at the engine.

1. Open the Group Policy Editor on the Windows computer by typing **gpedit.msc** in the Run line or Search box and pressing Enter. The Local Group Policy Editor window appears.
2. Navigate the tree to reach the following location: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
3. Under the Policy table, locate the policy entitled **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** (Figure 14).

Figure 14: FIPS Setup Window

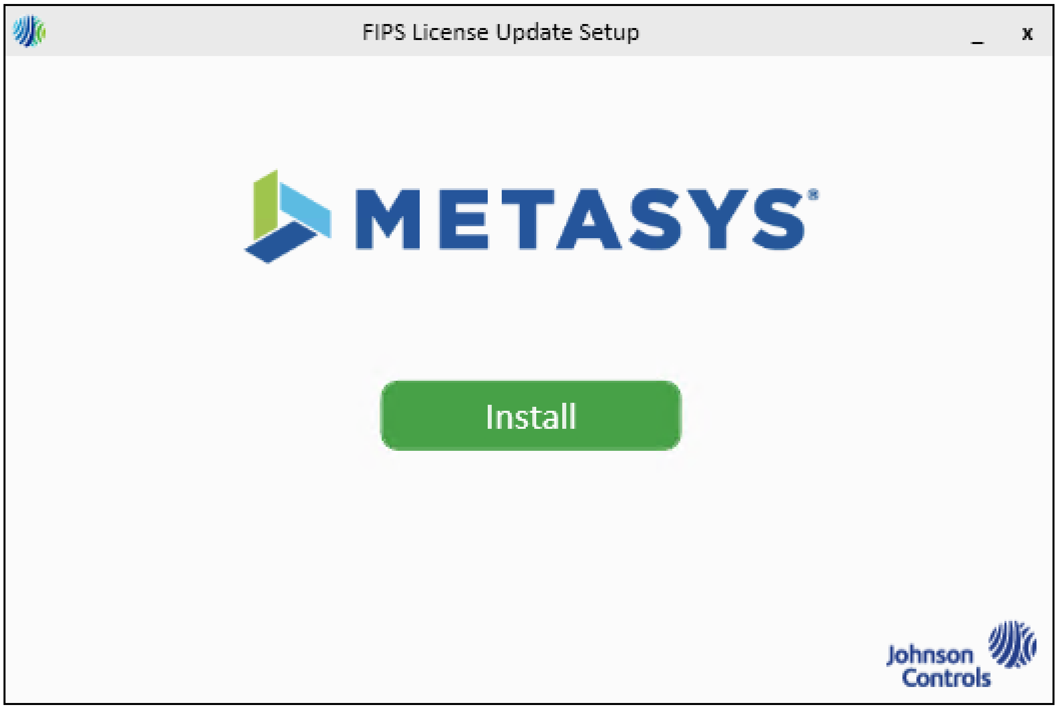

Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypt
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypt
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traf...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in thi...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to r...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	

4. Right-click this policy and select **Properties**. Select **Enabled** and click **OK**. FIPS mode is now enabled.
5. Start Software Manager and activate the Metasys FIPS license. For details, refer to the *Software Manager Help (LIT-12012389)*.
6. Obtain the Metasys FIPS installation file.
7. Using Windows Explorer, browse to the location of the Metasys FIPS installation file.

8. Right-click **MetasysFipsInstaller.exe** and select **Run as Administrator**. Enter the Administrator's user credentials if prompted. The setup window appears.

Figure 15: FIPS Setup Window



9. To continue, click **Install**. The progress of each step is shown.
10. After all installation steps have finished, click **Finish**.
11. To verify the FIPS component is now licensed, log on the Metasys SMP and open the Focus window for the ADS object. Verify the FIPS Compliance Status attribute indicates **Compliant (Licensed)**.

Uninstalling and unlicensing FIPS component

Follow the steps in this section if the customer requires you to uninstall and unlicense the FIPS component on the Metasys Server .

- **Important:** Before you uninstall the FIPS component (FIPS License Update) from the Metasys Server, you **must**uninstall the Metasys Server first. See Uninstalling Metasys Server Software.
- **Important:** After you disable FIPS on your Metasys Server , all network engines on the site that were updated to Release 11.0 remain FIPS compliant, which is an inherent feature of all network engines at Release 11.0. These network engines continue to function normally with a Metasys Server that is not FIPS compliant.

1. Uninstall the Metasys Server software. For details, see Uninstalling Metasys Server Software.
2. Open the Group Policy Editor on the Windows computer by typing **gpedit.msc** in the Run line or Search box and pressing Enter. The Local Group Policy Editor window appears.
3. Navigate the tree to reach the following location: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
4. Under the Policy table, locate the policy entitled **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.

5. Right-click this policy and select **Properties**. Select **Disabled** and click **OK**. FIPS mode is now disabled.
6. Start Software Manager and deactivate the FIPS license. For details, refer to the *Software Manager Help (LIT-12012389)*.
7. Uninstall the Metasys FIPS component from the Metasys Server computer by following these steps:

   a. In Control Panel, click **Programs > Programs and Features**.

   b. Select the **FIPS License Update**program item with Johnson Controls PLC shown as the Publisher.

   c. Click **Uninstall**, then follow the wizard uninstallation steps.

8. Reinstall the Metasys Server software. For details, see the default or custom installation methods under Metasys Server Software.
9. To verify the FIPS component is now unlicensed, log on the Metasys SMP and open the Focus window for the ADS object. Verify the FIPS Compliance Status attribute indicates **Non-Compliant (Unlicensed)**.

Installing Microsoft Silverlight 5

About this task:

ⓘ **Note:** The Microsoft® Silverlight® 5 plug-in (or later) is required to view Graphics+ files within the SMP UI that were created with the Graphic Generation Tool. If you choose to not install Microsoft Silverlight 5 (or later), you can view Graphics+ graphics associated with spaces or equipment in the Metasys UI. If this facility does not use Graphics+ files, go to the next section Launching the User Interfaces.

1. Go to the following website: http://www.microsoft.com/Silverlight.
2. Click **Download Now**.
3. Click **Run** to start the installation of Silverlight.
4. Click **Install now**.
5. Go to Launching the User Interfaces.

MVE Software

Important: You must purchase and license the Metasys Server (ADX) in addition to MVE. ADX with MVE installation requires you to install or upgrade an ADX, and then install MVE to enable the MVE functionality.

To install or upgrade to an ADX with MVE, you must have the following items:

- A supported server-class operating system
- A supported version of SQL Server software, Standard or Enterprise edition
- ADX installation file downloaded from the License Portal
- MVE installation file downloaded from the License Portal

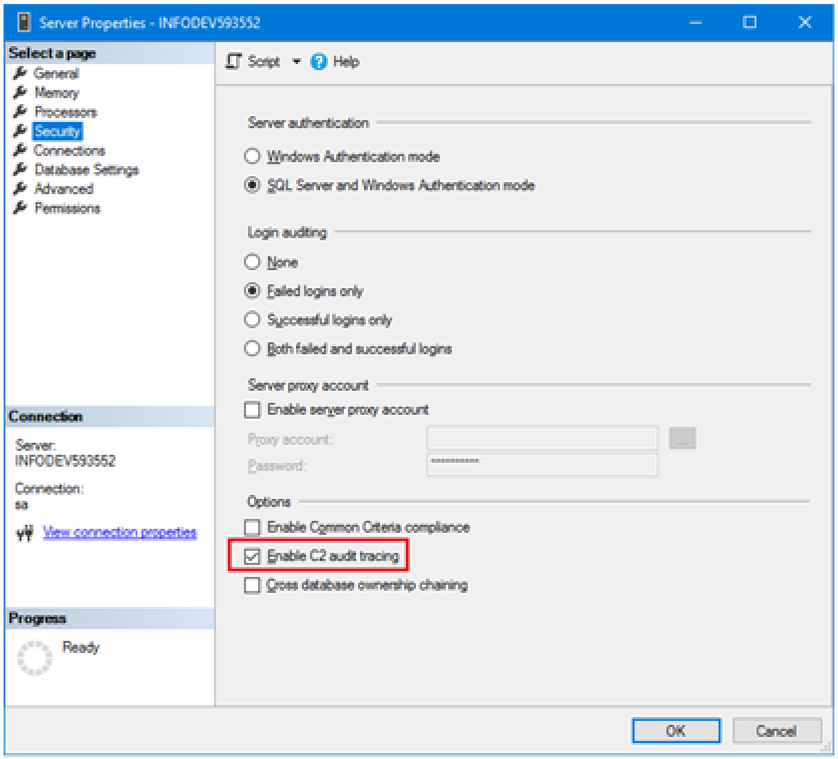
Consider the following for an ADX with MVE:

- After you install or upgrade an ADX, add MVE by running the MVE installer.

- MVE supports either a unified and or split ADX installation. Also see Split ADX for additional rules when installing on a split ADX.
- MVE supports the Metasys Advanced Reporting System. See Metasys Advanced Reporting System (ADX/ODS Only).

ⓘ **Note:** As part of installing MVE software, the MVE installer automatically enables the C2 Audit Tracing feature in SQL Server, as shown below. Selecting this option configures SQL Server to record in a log file all failed and successful attempts to access statements and objects. Information in the log file helps you investigate system activity and track possible security policy violations. However, the C2 audit tracing feature in SQL Server creates auditing files that grow rapidly. If left enabled and not maintained, C2 audit tracing can greatly reduce available disk space where SQL Server is installed, even to the point of causing a shutdown of SQL Server, or the computer itself to run out of disk space and then shut down. Therefore, if you do not need this feature, disable C2 auditing. Or, if you ever uninstall MVE, you must remember to disable it.

Figure 16: MVE installer checks Enable C2 audit tracing attribute in SQL Server



Server Properties - INFODEV593552

Server authentication

○ Windows Authentication mode
● SQL Server and Windows Authentication mode

Login auditing

○ None
● Failed logins only
○ Successful logins only
○ Both failed and successful logins

Server proxy account

□ Enable server proxy account
Proxy account:
Password: ***********

Options

□ Enable Common Criteria compliance
☑ Enable C2 audit tracing
□ Cross database ownership chaining

Connection
Server:
INFODEV593552
Connection:
sa

Progress
Ready

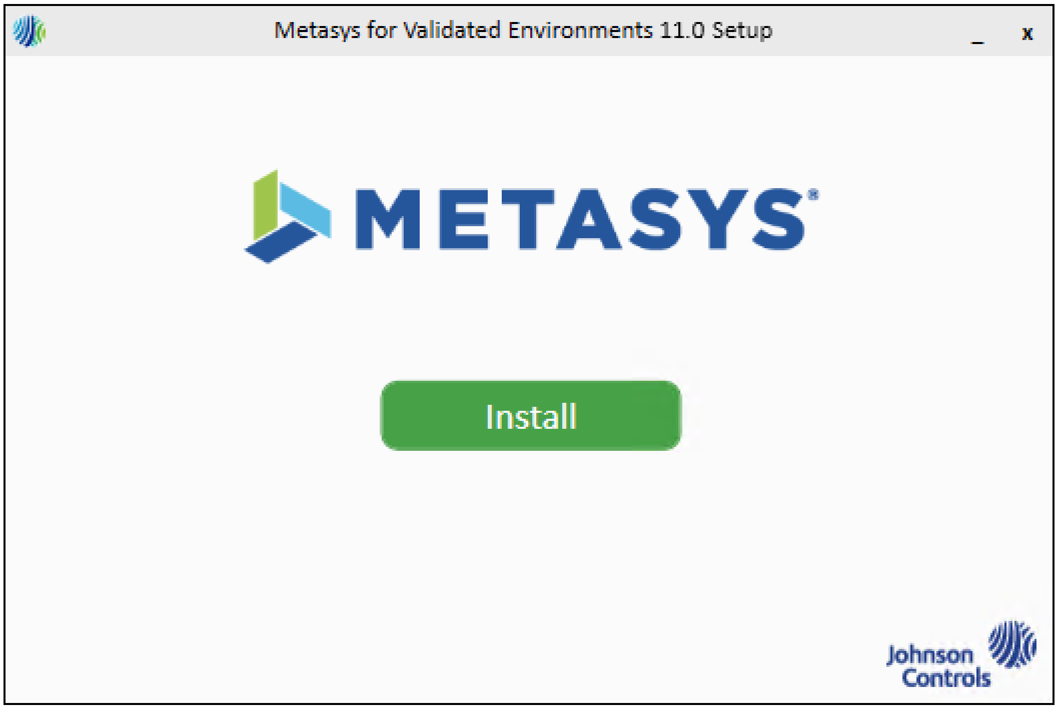
Installing MVE Software

About this task:

ⓘ **Note:** If a previous release of MVE software is installed on your computer, you must first uninstall it. Go to Uninstalling MVE Software.

1. Obtain the MVE installation file.
2. Using Windows Explorer, browse to the location of the MVE installation file.
3. Right-click **MetasysValidationEnvironment_11.0.exe** and select Run as Administrator. Enter the Administrator's user credentials if prompted. The setup window appears.
4. On the Setup window, click **Install**.

Figure 17: Welcome Screen



5. Under the Database section, select from these options:

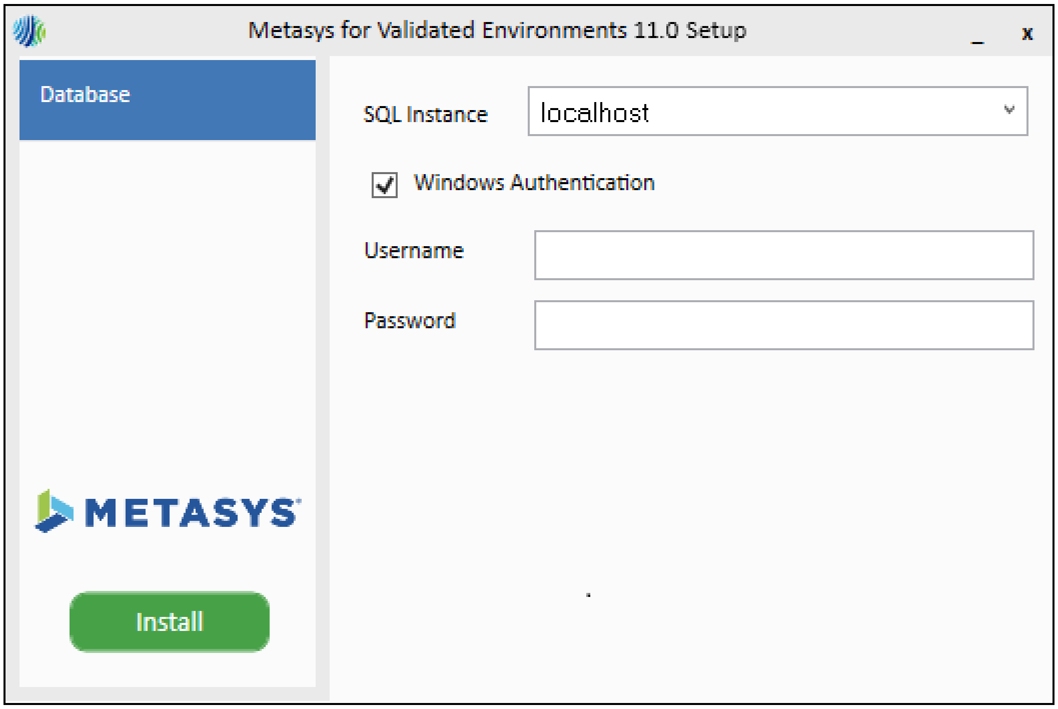
   a. **SQL Instance**: Click the down arrow to select the server name of the SQL database engine installed on the computer. For a unified ADX, you select **(localhost)** in most cases. However, if multiple SQL Server instances are found on the local server, click the one to use for Metasys software. For a split ADX, input the database server name in this format: `<servername>` (default instance) or `<servername>\<database instance>` (named instance).

      ⓘ **Note:** If your installation of SQL Server uses the default instance name, specify only the server name, but do not include the default instance name. Otherwise, an error message appears and you cannot proceed with the installation. You only need to specify a database instance if you have a named instance. Also, if the server name you specify does not resolve, use the server's IP address.

   b. **Windows Authentication**: Select if you want the installer to use the Windows OS credentials of the currently logged-in user to access the SQL Server software. The logged-in user **must be** a member of the system administrators (sysadmin) role in SQL Server. After installation, you can remove the SQL Server software system administrator rights from this user if so directed by IT personnel.

   c. **Username** and **Password**: Clear the **Use Windows Credentials** box to enter the SQL Server Administrator login and password credentials in these fields if you want the installer to use a SQL Server login with system administrator rights.

Figure 18: Database Screen



SQL Instance: localhost

☑ Windows Authentication

Username:

Password:

6. Click **Install**. The installer begins. The progress of each step is shown. This process takes less than a minute to complete. After all installation steps have finished, the Metasys Validation Environment Setup Complete box appears that offers either of two options:

   - **Restart Now**: a restart is needed to make the changes on your computer, such as enabling in C2 audit tracing in SQL Server. Click **Restart Now**, then after the restart, continue with the next step.
   - **Finish**: a restart is not needed. Click **Finish** and proceed to the next step.

7. License the MVE software with the Software Manager. For licensing instructions, refer to the *Software Manager Help (LIT-12012389)*.

Launching the User Interfaces

This section covers the launching of the user interfaces that are installed with the Metasys Server software: Site Management Portal (SMP) UI, Metasys Advanced Reporting System UI (ADX only), and the Metasys UI.

- To launch the SMP UI: see Launching the ADS/ADX SMP UI for instructions.
- To launch the Metasys Advanced Reporting System (ADX only): see Launching the Metasys Advanced Reporting System UI.
- To launch the Metasys UI: see Launching the Metasys UI.

If you want to secure the launching of the SMP UI with the Warning Banner option, refer to *Metasys Site Management Portal Help (LIT-1201793)* for details on how to enable the Warning Banner option.

ⓘ **Note:** We strongly recommend that you do not browse to the SMP UI from a computer running a server-class OS. By default, Windows Internet Explorer Enhanced Security Configuration is enabled on server-class operating systems, and may block the Launcher download page from access to the SMP. Open the SMP UI from a computer that is not running a server-class OS.

Launching the ADS/ADX SMP UI

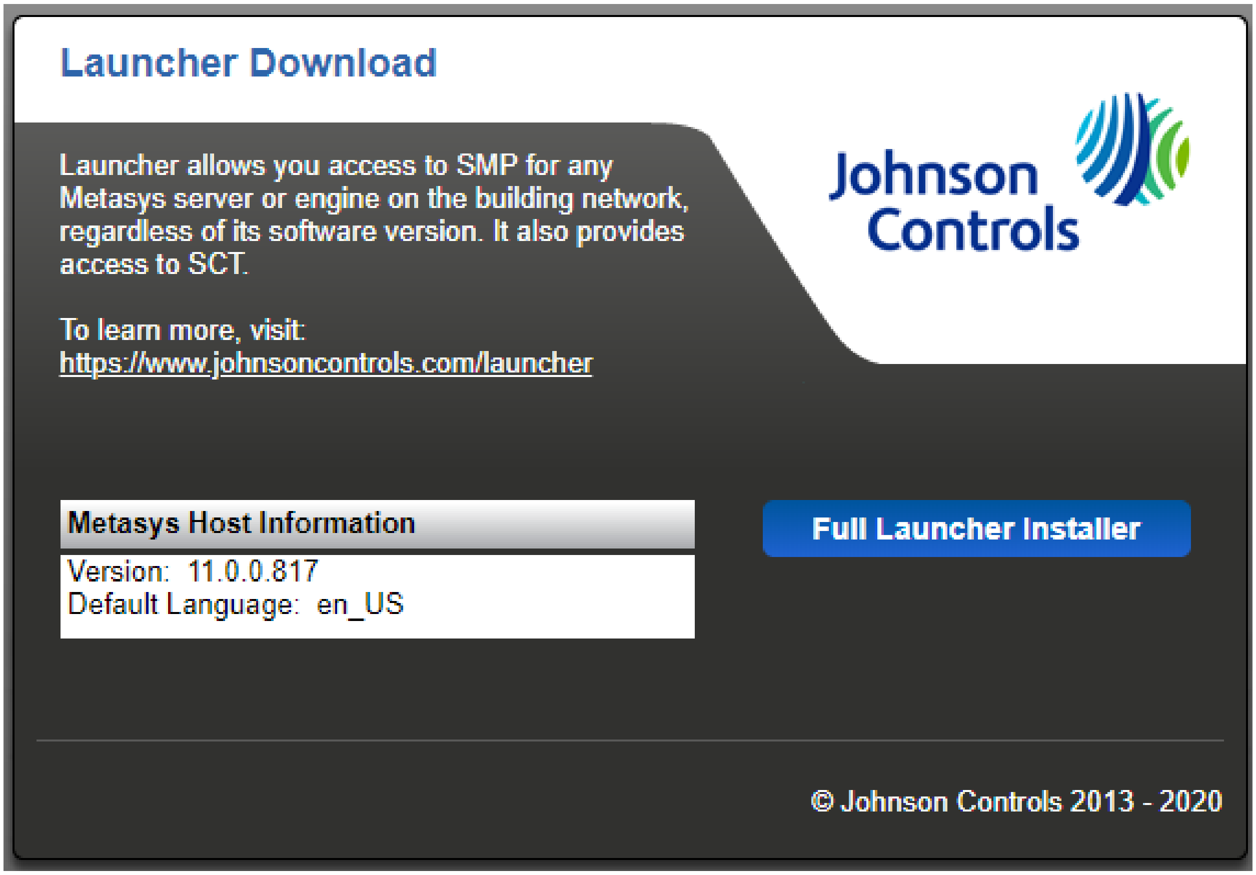
To launch the ADS/ADX SMP UI, do one of the following:

- On the ADS/ADX computer, from the Windows Start icon, go to **Johnson Controls** > **Launcher**. Follow the steps in *Launcher Tool Help (LIT-12011742)* to add a profile for the ADS/ADX under the SMP tab.
- On the ADS/ADX computer, double-click the **Metasys ADS** or **Metasys ADX** icon on the desktop. Add a profile for ADS/ADX under the SMP tab by configuring the network credentials of the ADS/ADX computer. For details, refer to *Launcher Tool Help (LIT-12011742)*.
- On another computer on the same network as the ADS/ADX computer, browse to **https://<hostname>/metasys/**, where **<hostname>** is the computer name of the target ADS/ADX.

  ⓘ **Note:** If the message **Missing Resource File** appears when you try to open the ADS/ADX, prompt the server to push its version of the Launcher by browsing to **https://<hostname>/launcher.msi.**

When you browse to the ADS/ADX computer from a client for the first time, the Windows Launcher Download screen appears (Figure 19). Click **Full Launcher Installer** to retrieve the user interface files (that is, a private version of the JRE) from the ADS/ADX computer, and then run the Launcher installation file. For details, refer to the *Launcher Installation Instructions (LIT-12011783)*.

Figure 19: Launcher Download Screen



Launcher Download

Launcher allows you access to SMP for any Metasys server or engine on the building network, regardless of its software version. It also provides access to SCT.

To learn more, visit:
https://www.johnsoncontrols.com/launcher

Metasys Host Information

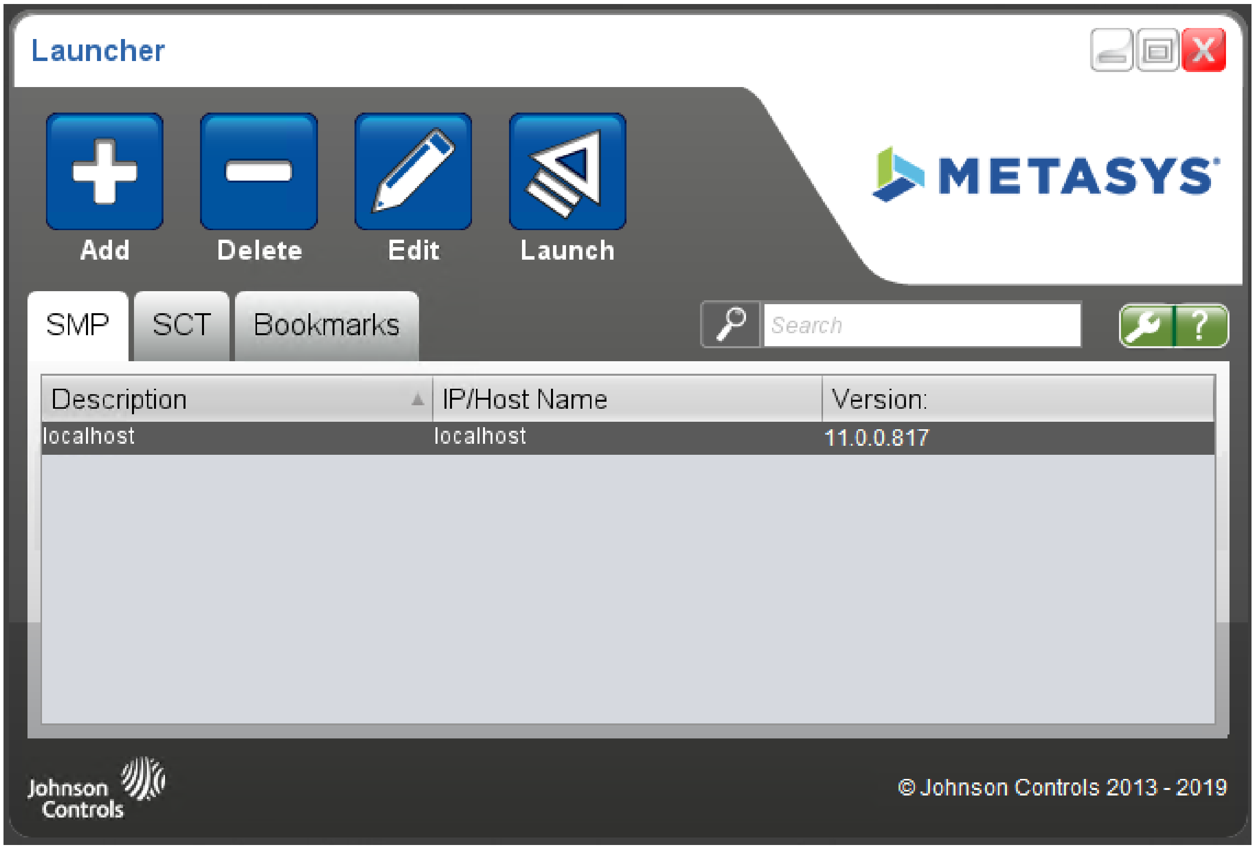
Version: 11.0.0.817
Default Language: en_US

© Johnson Controls 2013 - 2020

ⓘ **Note:** After you install the Launcher, use the Launcher, not the web browser, to access the ADS/ADX. If you use the web browser, the Launcher Download screen appears again. Do not reinstall the Launcher.

After you install the Launcher to your local hard drive, the Main Screen of the Launcher appears on which you can configure the network credentials of the ADS/ADX computer (Figure 20).

Figure 20: Launcher Main Screen



Description	IP/Host Name	Version:
localhost	localhost	11.0.0.817

Using the Launcher, configure the network credentials of the ADS/ADX computer to add its profile to the Launcher. For details, refer to the *Launcher Tool Help (LIT-12011742)*.

After you add the ADS/ADX, select it from the profile list under the SMP tab and click **Launch**. The SMP UI login screen appears. Log in with the MetasysSysAgent user name and default password. (For the default password, contact your local Johnson Controls representative.) You are forced to change the password to a valid, complex password the first time you log in to the ADS/ADX. Follow the password rules that appear in the Change Password dialog. For more information on passwords, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

For information on configuring and using ADS/ADX, refer to the *ADS/ADX Commissioning Guide (LIT-1201645)* and *Metasys Site Management Portal Help (LIT-1201793)*.

Launching the Metasys Advanced Reporting System UI

You must log in to the ADX SMP UI and accept the license agreement before you access the Metasys Advanced Reporting System UI. This applies only to the first time you log in to the reporting system after an install or upgrade. See Launching the User Interfaces.

To launch the Metasys Advanced Reporting System UI, do one of the following:

- In the SMP UI, select **Tools** > **Advanced Reporting**.
- In Internet Explorer 11 or Microsoft Edge, browse to https://**<hostname>/MetasysReports**, where **<hostname>** is the computer name of the target ADX.

ⓘ **Notes:**

- In Internet Explorer 11, select the **Use Microsoft compatibility lists** option, under **Tools** > **Compatibility View Settings**, to ensure that websites appear and function correctly.
- Metasys Advanced Reporting System and Energy Essentials support Internet Explorer 11 on all computer platforms except on Windows 10. On Windows 10 computers, both Internet Explorer 11 and Microsoft® Edge® are supported.

- Add the web address of the Metasys Advanced Reporting System to the Launcher, and use the Launcher to start the Metasys Advanced Reporting System UI.

Launching the Metasys UI

To access the Metasys UI remotely from any client device, ensure that you have access to the Metasys Site Director (Internet, intranet, or Virtual Private Network (VPN) access) and browse to **https://[SERVERNAME]/UI**, where [SERVERNAME] is replaced with the hostname or IP address of your Metasys Site Director.

When you browse to the Metasys UI, your web browser displays a security certificate warning. The browser displays this warning if your Metasys UI site does not have a trusted security certificate.

If you see this warning, you can browse to the Metasys UI site by doing the following:

- For Google Chrome, (1) tap or click **Advanced**; (2) Tap or click **Proceed to [IP Address]**, where [SERVERNAME or IP Address] is the server name or IP address of the Site Director.
- For Windows Internet Explorer, click **Continue to this website (not recommended)**.
- For Microsoft Edge, click **Continue to this website (not recommended)**.
- For Apple Safari, tap or click **Continue** in the Cannot Verify Sever Identity window.

The Metasys UI login screen appears. Enter your Metasys SMP login credentials.

Appendix: Windows firewall

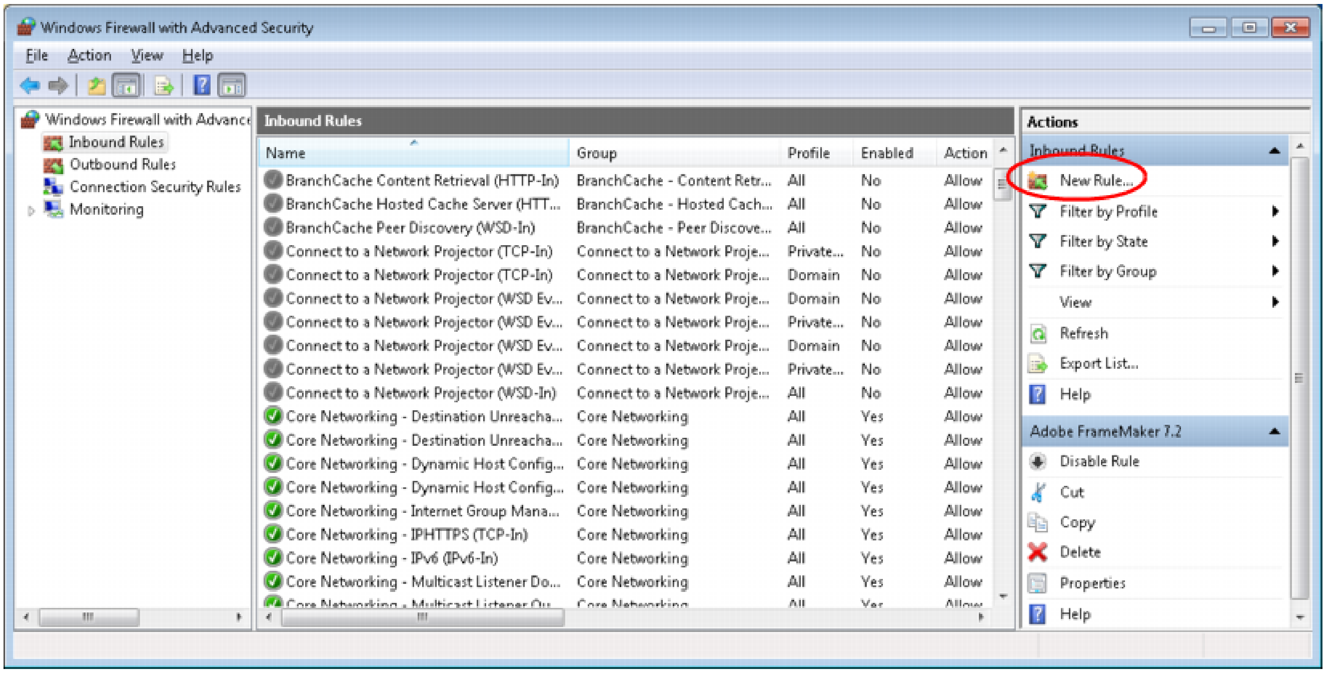
As a best practice, enable the Windows Firewall as indicated in this section, but always follow the recommendation of the customer's local IT staff. Some customers may not require enabling the Windows Firewall.

Configuring the Windows firewall

About this task:
As a best practice, enable the Windows Firewall as indicated in this section, but always follow the recommendation of the customer's local IT staff.

1. In Control Panel, click **System and Security**, then click **Windows Firewall**. The Windows Firewall window appears.
2. In the Windows Firewall window, make sure the firewall is **On**. If not, turn on the Windows Firewall.
3. Click **Advanced Settings**. The Windows Firewall with Advanced Security window appears.
4. In the left pane, click **Inbound Rules**. The Inbound Rules pane appears.

Figure 21: Windows Firewall - Inbound Rules



Name	Group	Profile	Enabled	Action
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow

5. In the Actions pane, select **New Rule**. The New Inbound Rule Wizard opens and the Rule Type window appears.
6. Select **Port** and click **Next**. The Protocol and Ports window appears.
7. Select **TCP**, and in the **Specific Local Ports** field, enter the port numbers (25, 80, 88, 110, 135, 389, 443, 445, 465, 587, 995, 1025, 1433, 2103, 2105, 3389, 5291, 5960, 9910, 10050, 12000).

Table 48: Ports to Open for TCP Protocol

Protocol	Port
SMTP	25
HTTP	80
Kerberos	88
POP3	110
Remote Procedure Call (RPC)	135
LDAP	389
HTTPS (TLS)	443
NT LAN Manager Version 2 (NTLMv2)	445
SMTP over TLS	465
SMTP	587
POP3 over TLS	995
Remote Procedure Call (RPC)	1025
Microsoft SQL Server Database	1433
RPC over TCP	2103
RPC over TCP	2105
Microsoft Terminal Server	3389
(Unassigned)	5291

Table 48: Ports to Open for TCP Protocol

Protocol	Port
(Unassigned)	5960
Microsoft Discovery Protocol	9910
Zabbix Agent	10050
(Unassigned)	12000

8. Click **Next**. The Action window appears.
9. Select **Allow the connection**. Click **Next**. The Profile window appears.
10. Keep all profile check boxes selected (default). Click **Next**. The Name window appears.
11. Specify **Metasys (TCP Protocol)** as the name. Optionally, you can add a description to identify this new rule. Click **Finish**.

    The Inbound Rules table refreshes to indicate the new rule called Metasys (TCP Protocol). Ports 25, 80, 88, 110, 135, 389, 443, 445, 465, 587, 995, 1025, 1433, 2103, 2105, 3389, 5291, 5960, 9910, 10050, 12000 are now open and ready for use.
12. Repeat Step 5 through Step 11 to add a new Metasys inbound rule for the UDP protocol. When the Protocol and Ports window appears, select **UDP**, and in the Specific Local Ports field, enter the port numbers (25, 53, 67, 68, 69, 88, 123, 161, 162, 9910, 9911, 47808).

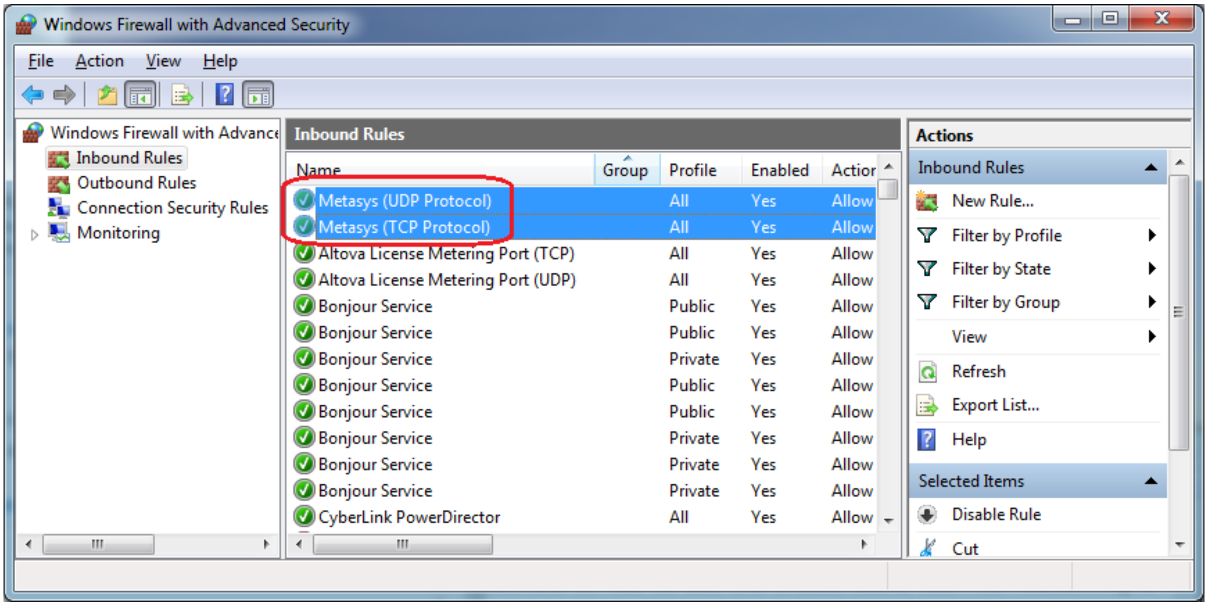
Table 49: Ports to Open for UDP Protocol

Protocol	Port
SMTP	25
DNS	53
DHCP	67
DHCP	68
Trivial File Transfer Protocol (TFTP)	69
Kerberos	88
Network Time Protocol (NTP)	123
SNMP	161
SNMP Trap	162
Microsoft Discovery Protocol	9910
SYPE-Transport	9911
BACnet®	47808, Configured for each supervisory device, including OAS, ODS and the NAE8500, in the Network Port Ethernet IP Datalink object

13. Complete the steps to add the new inbound rule. Name the new rule **Metasys (UDP Protocol)**.

    When finished, the **Windows Firewall with Advanced Security** window appears and the Inbound Rules table refreshes to indicate the new rule called **Metasys (UDP Protocol)**. Ports 25, 67, 68, 69, 53, 88, 123, 161, 162, 9910, 9911, and 47808 are now open and ready for use.
14. In the **Windows Firewall with Advanced Security** window, verify that the two new Metasys inbound rules are defined and enabled.

Figure 22: Metasys Inbound Rules Defined and Enabled



Name	Group	Profile	Enabled	Actior
Metasys (UDP Protocol)		All	Yes	Allow
Metasys (TCP Protocol)		All	Yes	Allow
Altova License Metering Port (TCP)		All	Yes	Allow
Altova License Metering Port (UDP)		All	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Private	Yes	Allow
CyberLink PowerDirector		All	Yes	Allow

15. Close the **Windows Firewall with Advanced Security** window.
16. Close all windows.

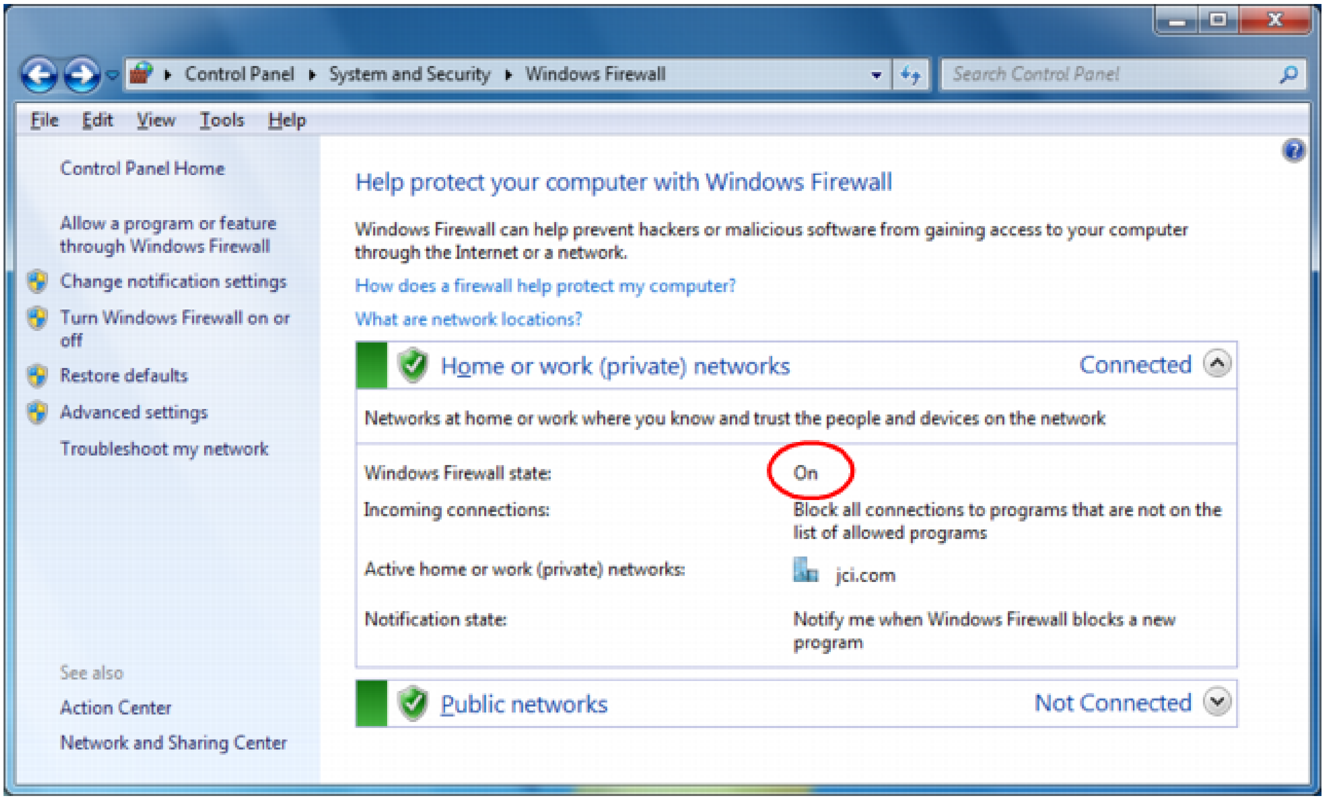
Closing ports

About this task:
This section provides an overview on how to close ports if desired. Note that closing ports can have unforeseen effects on other parts of your system. The example in this section shows blocking inbound Port 80; you can block outbound Port 80 as well by defining an outbound rule, although the ADS/ADX/ODS and network engines do not communicate out of Port 80.

ⓘ **Note:** The latest available version of the ODS is Release 10.1. The ODS is not available for upgrade to Metasys Release 11.0.

1. In Control Panel, click **System and Security**, then click **Windows Firewall**. The Windows Firewall window appears.
2. In the Windows Firewall window, make sure the firewall is **On**. If not, turn on the Windows Firewall.

Figure 23: Windows Firewall



Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
File Edit View Tools Help

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	jci.com
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

3. Click **Advanced Settings** in the left pane. The Windows Firewall with Advanced Security window appears.
4. In the left pane, click **Inbound Rules**. The Inbound Rules pane appears.
5. In the Actions pane, select **New Rule**. The New Inbound Rule Wizard opens and the Rule Type window appears.
6. Select **Port** and click **Next**. The Protocol and Ports window appears.
7. Select **TCP**, and in the Specific Local Ports field, enter the port numbers you want to close. This example shows Port 80.
8. Click **Next**. The Action window appears.
9. Select **Block the connection** and click **Next**.
10. Complete the steps to add the new inbound rule. Name the new rule **Metasys (TCP Protocol Closed Ports), BCM (TCP Protocol Closed Ports)**.

    When finished, the Windows Firewall with Advanced Security window appears and the Inbound Rules table refreshes to indicate the new rule called **Metasys (TCP Protocol Closed Ports) BCM (TCP Protocol Closed Ports)**. The ports you specified in **Step 7** are now closed to inbound traffic.

11. In the Windows Firewall with Advanced Security window, verify that the new Metasys inbound rule is defined and enabled.
12. If you also need to close UDP ports, select **New Rule** from the **Actions** menu and repeat steps 5 through 11, substituting UDP for TCP in **Step 7**. You can also create a new outbound rule if you want to block outgoing traffic over a particular port. In that case, select the Outbound Rules option in **Step 4**.
13. Close the Windows Firewall with Advanced Security window.
14. Close any additional windows.

Appendix: Certificate management and security

Follow the steps in this appendix for managing the trusted certificates on the Metasys Server or SCT computer, and for selecting security levels for the site. The Metasys server, SCT computer, and network engines are installed with self-signed certificates, which enables encrypted network communication between the devices. Optionally, the customer can deploy trusted certificates at the Metasys server or SCT computer and enable encrypted and trusted communication between the Metasys server and network engines. Trusted certificates, installed on the client computer and the Metasys SMP or SCT computer, are either provided by the customer's IT department or a Certificate Authority (CA). A security shield icon on the Metasys server or SCT login and user interface screens indicate the encryption state:

- **Green Shield**: the connection is encrypted and trusted
- **Orange Shield**: the connection is encrypted, but not trusted
- **Red Shield**: the connection is encrypted, but the security level cannot be verified

To deploy a trusted server certificate at the Metasys server or SCT computer, follow **Steps 1-3** referenced below. Then, if the IT department or CA has provided separate files for the root and intermediate certificates, follow **Step 4**. Also follow **Step 4** if you need to establish a trusted relationship between the client computer and the Metasys server and SCT computer. If you want to establish **encrypted and trusted** communication between the Metasys server and network engines, follow **Step 5**, which explains how to set the Site Security Level. Lastly, perform **Step 6** if you want to verify all certificates are in place.

1. Requesting a server certificate
2. Completing a server certificate request
3. Binding the secure certificate
4. Importing root and intermediate certificates
5. Setting the Site Security Level to Encrypted and Trusted
6. Verifying the server certificate chain

For details on how to remove or rebind a secure certificate, see Removing or rebinding the secure certificate. For details about how to remove a self-signed certificate from the certificate store, see Removing the self-signed certificates in the certificate store. For details on renewing an existing certificate, see . For details about managing certificates on network engines, refer to *Metasys SCT Help (LIT-12011964)*.

Lastly, this appendix describes how to use two special security attributes that you set in the site object of the Site Director: Site Security Level and Advanced Security Enabled. See the following sections for details:

Setting the Site Security Level to Encrypted and Trusted

Changing Advanced Security Enabled to False

Requesting a server certificate

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Under the IIS section in the middle pane, double-click **Server Certificates**. The Server Certificates panel appears.

3. On the Actions pane, click **Create Certificate Request**. The Distinguished Name Properties screen appears.
4. Fill out all the fields in the form. For Common name, specify the full computer name, which you can determine from ***Control Panel*** > ***System and Security*** > ***System***. The full name may also include a domain name (for example, MAIN-ADX.mycorp.com). Click **Next**. The Cryptographic Service Provider Properties screen appears.
5. Select an appropriate service provider and bit length. Click **Next**. The File Name screen appears.
6. Click the **Browse (...)** button to select a location where to save the certificate request file. The Specify Save as File Name window appears.
7. Type in a file name and click **Open**. The File Name window appears with the file name specified.
8. Click **Finish**. The certificate request file with a .txt extension is created in the selected folder. For example, the certificate request file for a server called MAIN-ADX would be **MAIN-ADX.txt**.
9. Send the certificate request file to the IT department or CA to obtain your trusted certificate. When you receive the file, go to Completing a server certificate request to import the certificate into the server.

Completing a server certificate request

About this task:
To complete a certificate request for a Metasys server or SCT computer:

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Under the IIS section in the middle pane, double-click **Server Certificates**. The Server Certificates panel appears.
3. On the Actions pane, click **Complete Certificate Request**. The Specify Certificate Authority Response screen appears.
4. Use the browse button to locate the certificate that your IT department provided. Specify a friendly name for the server. Select **Personal** under **Select a certificate store for the new certificate** if this field appears. Click **OK** to complete the certificate request. The Server Certificates window appears indicating the new certificate has been imported.
5. Next, you need to bind the certificate. See Binding the secure certificate.

Binding the secure certificate

About this task:
To bind a secure certificate for a Metasys server or SCT computer:

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Expand the Connections in the left pane so that Default Web Site appears. Click **Default Web Site**.
3. On the Actions pane, click **Bindings** under Edit Site. The Site Bindings screen appears.
4. Click **Add**. The Add Site Bindings screen appears.
5. Under Type, select **https**. Under SSL certificate, select the name of the server certificate you imported in Completing a server certificate request. Click **OK**.

ⓘ **Note:** Make sure that proper certificate revocation, such as Online Certificate Status Protocol (OCSP) stapling, is enabled and configured. For more information about OCSP configuration refer to https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-ocsp/5792b4c4-c6ba-439a-9c2a-52867d12fb66

6. If you need to import root and intermediate certificates of the Metasys Server or SCT computer at a client computer, go to Importing root and intermediate certificates. This step is necessary if you want the green shield icon to appear on Metasys SMP and SCT login and user interface screens.

   If you want to skip that step and you want to verify the certificate chain you created in the previous sections, see Verifying the server certificate chain.

Importing root and intermediate certificates

About this task:
Follow these steps to import root and intermediate certificates of a Metasys server or SCT computer at the client computer (that is, the computer that remotely logs in to SMP or SCT). Also perform these steps to import certificates when the IT department or CA provided separate files for the root and intermediate certificates.

1. Start the Microsoft Management Console at the client computer by typing `mmc` in the Search bar and pressing **Enter**. The Microsoft Management Console screen appears.
2. Click ***File*** > ***Add/Remove Snap-ins***. The Add or Remove Snap-ins screen appears.
3. Under the Available snap-ins list, select **Certificates** and click **Add**. The Certificate Snap-in screen appears.
4. Select **Computer account** and click **Next**. The Select Computer screen appears.
5. Click **Local computer** and click **Finish**. The Add or Remove Snap-ins screen appears indicating the Certificates addition.
6. Click **OK.** The Microsoft Management Console window appears with the Certificates snap-in.
7. Select **Trusted Root Certification Authorities**. Under More Actions, click ***All Tasks*** > ***Import***. The Certificate Import Wizard appears.
8. With Local Machine pre-selected, click **Next**. The next screen prompts you for the location of the certificate file request. Select the certificate request file, using the Browse button to help locate the file. Click **Next**.
9. Select **Trusted Root Certificate Authorities** as the location where to store the certificate. Click **Next**.
10. Click **Finish** to complete the certificate import.
11. Under ***Trusted Root Certificate Authorities*** > ***Certificates***, verify the root certificate has been imported.
12. Repeat the steps in this section for importing any required intermediate server certificates as necessary, but in Step 7, select the **Intermediate Certification Authorities** as the certificate type.

Verifying the server certificate chain

About this task:
To verify a certificate chain for a Metasys server or SCT computer:

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Highlight the name of the web server.

3. Under the IIS section in the middle pane, double-click **Server Certificates**. The Server Certificates panel appears.
4. On the Actions pane, click **View**. The Certificate screen appears.
5. Click the **Certification Path** tab. The certificate chain appears.
6. Click **OK** to close the certificate view.

Removing or rebinding the secure certificate

About this task:
Follow these steps to remove a certificate binding from a Metasys server or SCT computer or to change a certificate binding. If you are changing a binding, the binding must already exist on the server from which to select.

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Expand the Connections in the left pane so that Default Web Site appears. Click **Default Web Site**.
3. On the Actions pane, click **Bindings** under Edit Site. The Site Bindings screen appears.
4. To remove the site binding, select it from the list and click **Remove**. A user prompt appears to verify that you want to remove the selected binding. Click **Yes** to remove or **No** to cancel.

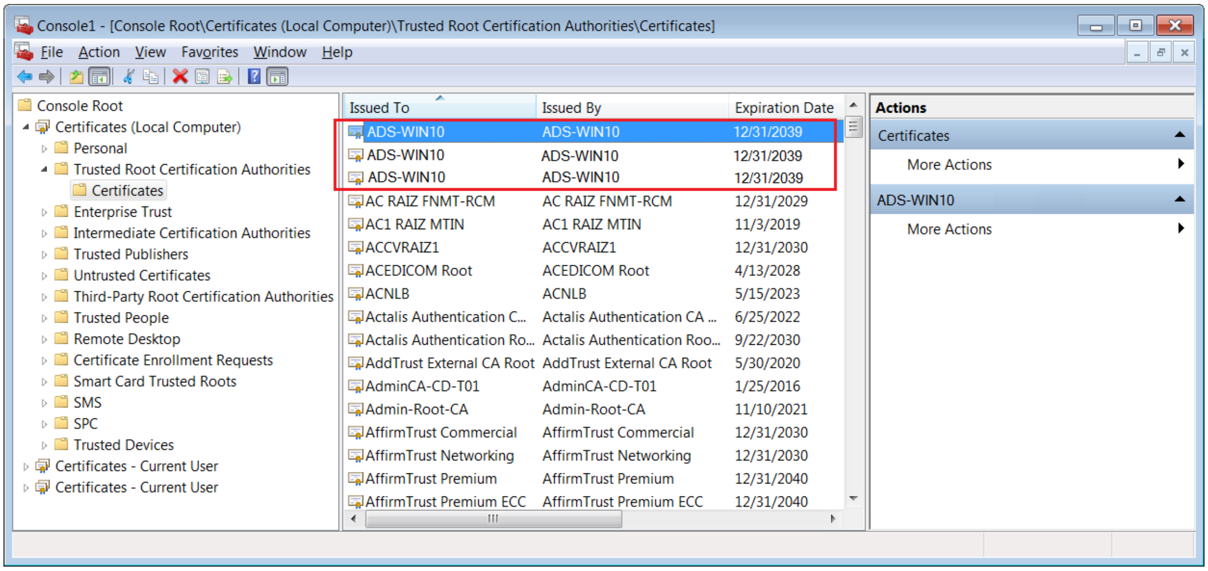
   To rebind the certificate, select it from the list and click **Edit**. The Edit Site Binding screen appears.
5. Click **Select** to open a table that lists all certificates available for binding.
6. Select the binding from the table and click **OK**. The Edit Site Binding screen appears with the newly selected binding.
7. Click **OK** to save the binding change.

Removing the self-signed certificates in the certificate store

About this task:
Follow this procedure to manually remove self-signed certificates before upgrading Metasys server software or SCT software for a computer that has been renamed as part of the upgrade.

1. Start the Microsoft Management Console at the Metasys server or SCT computer by typing **mmc** in the Search bar and pressing **Enter**. The Microsoft Management Console screen appears.
2. Click > ***File*** > ***Add/Remove Snap-ins***. The Add or Remove Snap-ins screen appears.
3. Under the Available snap-ins list, select **Certificates** and click **Add**. The Certificate Snap-in screen appears.
4. Select **Computer account** and click **Next**. The Select Computer screen appears.
5. Click **Local computer** and click **Finish**. The Add or Remove Snap-ins screen appears indicating the Certificates.
6. In the Add or Remove Snap-ins window, click **Add** again. The Certificate Snap-in screen appears again. This time, click ***My user account*** > ***Next*** > ***Finish***. The Add or Remove Snap-ins screen appears showing the two snap-ins you just added.
7. Click **OK**. The Microsoft Management Console window appears with the Certificates snap-in.
8. Expand **Trusted Root Certification Authorities**. Look for a certificate that matches the old name of the computer. Several identical certificates may be listed. In this example, three certificates for the computer called ADS-WIN10 are listed.

Figure 24: Removing Certificate - Selecting Certificates to Delete


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Actions
Certificates
More Actions
ADS-WIN10
More Actions

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - SPC
    - Trusted Devices
  - Certificates - Current User
  - Certificates - Current User

Issued To	Issued By	Expiration Date
ADS-WIN10	ADS-WIN10	12/31/2039
ADS-WIN10	ADS-WIN10	12/31/2039
ADS-WIN10	ADS-WIN10	12/31/2039
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	12/31/2029
AC1 RAIZ MTIN	AC1 RAIZ MTIN	11/3/2019
ACCVRAIZ1	ACCVRAIZ1	12/31/2030
ACEDICOM Root	ACEDICOM Root	4/13/2028
ACNLB	ACNLB	5/15/2023
Actalis Authentication C...	Actalis Authentication CA ...	6/25/2022
Actalis Authentication Ro...	Actalis Authentication Roo...	9/22/2030
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
AdminCA-CD-T01	AdminCA-CD-T01	1/25/2016
Admin-Root-CA	Admin-Root-CA	11/10/2021
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030
AffirmTrust Networking	AffirmTrust Networking	12/31/2030
AffirmTrust Premium	AffirmTrust Premium	12/31/2040
AffirmTrust Premium ECC	AffirmTrust Premium ECC	12/31/2040

9. Select trusted certificates with the old computer name and click the **Delete** button or select ***Action*** > ***Delete***. The trusted certificates are removed. The next step is to remove personal certificates.
10. Expand **Personal**. Look for a certificate that matches the old name of the computer. Several identical certificates may be listed.
11. Select personal certificates with the old computer name and click the **Delete** button or select ***Action*** > ***Delete***.
12. Close the Microsoft Management Console, optionally saving the Console settings.

Certificate management troubleshooting

The following table lists troubleshooting topics for certificate management.

Table 50: Certificate management troubleshooting

Error Message or Scenario	Solution or Workaround
When you set the Site object Site Security Level attribute to **Encrypted and Trusted** and then download the Site Director, all network engines reporting to the Site Director are modified to change their Site Security Level attribute to Encrypted and Trusted. If a network engine Site Security Level attribute is set to Encrypted and Trusted and does not have a trusted certificate, the network engine does not communicate to the Site Director.	To resolve this issue: 1. Login to the network engine's Site Management Portal in Expert mode. 2. Open the Focus tab of the network engine object. 3. Click **Edit**. 4. For the Site Security Level attribute, select **Encrypted Only**. 5. Click **Save**. 6. Verify the network engine comes online at the Site Director.

Setting the Site Security Level to Encrypted and Trusted

About this task:

You can set the **Site Security Level** offline with SCT or online with the Site Management Portal UI. To use the online method to set the Site Security Level to **Encrypted and Trusted**, follow these steps:

1. Log on the Site Management Portal of the Site Director.
2. Open the **Site View** for the Site Director.
3. With Advanced selected, click **Edit**.
4. Locate the **Site Security Level** attribute under the **Operational Data** section.
5. Click the down arrow and select **Encrypted and Trusted**.

   ⓘ **Note:** When you set the Site Security Level attribute in the Site object to **Encrypted and Trusted**, all network engines reporting to the Site Director are modified to change their Site Security Level attribute to Encrypted and Trusted. If a network engine Site Security Level attribute is set to Encrypted and Trusted but does not have a trusted certificate, communication between the Site Director and the network engine is lost because the Site Director now requires the engine to communication with a trusted certificate. Also, if sometime later you want to change a network engine's Site Security Level back to Encrypted Only, you need to log on the network engine directly.

   Before you set the Site object Site Security Level attribute to **Encrypted and Trusted**, verify that all network engines reporting to the Site Director have trusted certificates. If the network engines do not have trusted certificates, keep this attribute set to **Encrypted Only**.
6. Click **Save**. The server and engines across the entire site now use encrypted and trusted communication.
7. As an option, use SCT to upload the Site Director so that this change is reflected in the database archive.

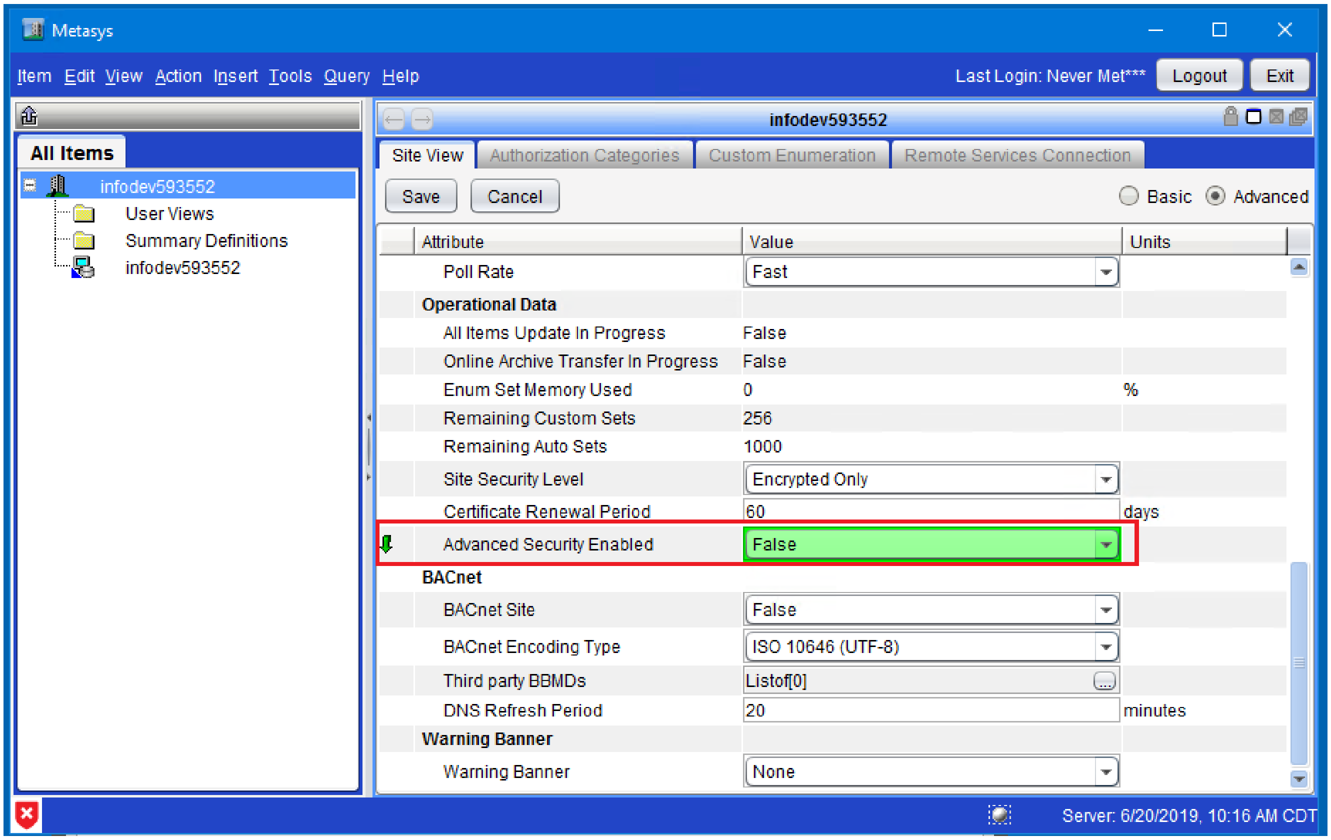
   If you want to later change the site to use encrypted only communication, repeat these steps but select **Encrypted Only**, then use SCT to upload the change to the archive.

Changing Advanced Security Enabled to False

About this task:
By default, the **Advanced Security Enabled** attribute on the Site object is set to **True** for the Metasys system installed at or upgraded to Release 11.0. This attribute provides an improved layer of security between Metasys Site Directors and devices. With this attribute set to true (default), older methods of secure communication between the Site Director and its network engines are disabled, which means a Site Director at Release 10.0 or later discards all communication attempts from network engines prior to Release 10.0. This setting applies to the entire site, so if you have any network engine on the site that is running a Metasys release prior to Release 10.0, use the steps in this section to change this Site object attribute to **False**. You can use either SCT (offline method) or the Site Management Portal UI (online method). To use the online method, follow these steps:

1. Log on the Site Management Portal of the Site Director.
2. Open the **Site View** for the Site Director.
3. With Advanced selected, click **Edit**.
4. Locate the **Advanced Security Enabled** attribute under the **Operational Data** section (Figure 25).
5. Click the down arrow and select **False**.

Figure 25: Changing the Advanced Security Enabled attribute



Attribute	Value	Units
Poll Rate	Fast	
Operational Data		
All Items Update In Progress	False	
Online Archive Transfer In Progress	False	
Enum Set Memory Used	0	%
Remaining Custom Sets	256	
Remaining Auto Sets	1000	
Site Security Level	Encrypted Only	
Certificate Renewal Period	60	days
Advanced Security Enabled	False	
BACnet		
BACnet Site	False	
BACnet Encoding Type	ISO 10646 (UTF-8)	
Third party BBMDs	Listof[0]	
DNS Refresh Period	20	minutes
Warning Banner		
Warning Banner	None	

6. Click **Save**. The server and engines across the entire site no longer use advanced security.
7. As an option, use SCT to upload the Site Director so that this change is reflected in the database archive.

   ⓘ **Note:** If sometime later you change the **Advanced Security Enabled** attribute from False to True, a user message appears to indicate that all network engines prior to Release 10.0 are disconnected from the site because they can no longer communicate with the Site Director using advanced security. Do not set **Advanced Security Enabled** to True until all network engines are upgraded to Release 10.0 or later.

Appendix: Special Features

The installation and upgrade of these special features is explained in detail elsewhere in this document. This section provides information you might want to know before you install, upgrade, or use the wizard.

See the following for more information:

- Split ADX
- Metasys Advanced Reporting System (ADX/ODS Only)
- Installing Metasys Server for a Non-English Locale
- Customizing Windows IIS for Metasys API
- Configuring Virtual Machine for Metasys Server

Split ADX

The split configuration of the ADX involves installing ADX functionality on two separate computers, with SCT on a third separate computer:

- **Web/application computer:** The computer where the **ADX software** is installed is known as the web/application server. The web/application server is where users browse to see system information.
- **Database computer:** The computer that contains the **SQL Server software database** is known as the database server. The database server houses historical data and cannot be used as a data repository by more than one web/application server.
- **SCT computer:** The computer that contains the **SCT software** is known as the SCT computer. You specify the name of the SCT computer on the Reporting tab when you select the Custom method of installing Metasys Server software. See Installing Metasys Server: Custom Method.

Note the following rules for split ADXs:

- In a split ADX configuration, the SCT must reside on its own computer; it cannot reside on either the web/application server or the database server.
- When you are installing the ADX software, the SCT computer and the database server must be accessible over the network to the web/application server.
- The appropriate SQL Server software components must be installed and running on the computer (or on both computers when installing the Metasys Advanced Reporting System) before you install the ADX software. ADX database configuration files automatically update with the database server path where the ADX is installed.
- A split ADX requires that the SQL Server login for the database server used during installation has a password that is not blank.
- A split ADX configuration always involves more than one physical computer or VM. For example, a computer where the ADX software is installed on one partition or disk drive and the SQL Server software is installed on a second partition or disk drive does not constitute a split ADX.
- Split ADXs with the Metasys Advanced Reporting System have special rules, regarding where to install SQL Server software. See Metasys Advanced Reporting System (ADX/ODS Only).

Metasys Advanced Reporting System (ADX/ODS Only)

During the ADX installation or upgrade process, you can add support for the Metasys Advanced Reporting System if you have the ADX installation file and the supported SQL Server software with SQL Server Database Services and Reporting Services. After you install an ADX, you **cannot** go back and add support for the Metasys Advanced Reporting System without reinstalling the ADX software.

The Metasys Advanced Reporting System supports unified ADX and split ADX installations.

The Metasys Advanced Reporting System supports the following configurations:

- Unified ADX with SCT on the ADX computer
- Split ADX with SCT on a third, separate computer

Consider the following for the Metasys Advanced Reporting System:

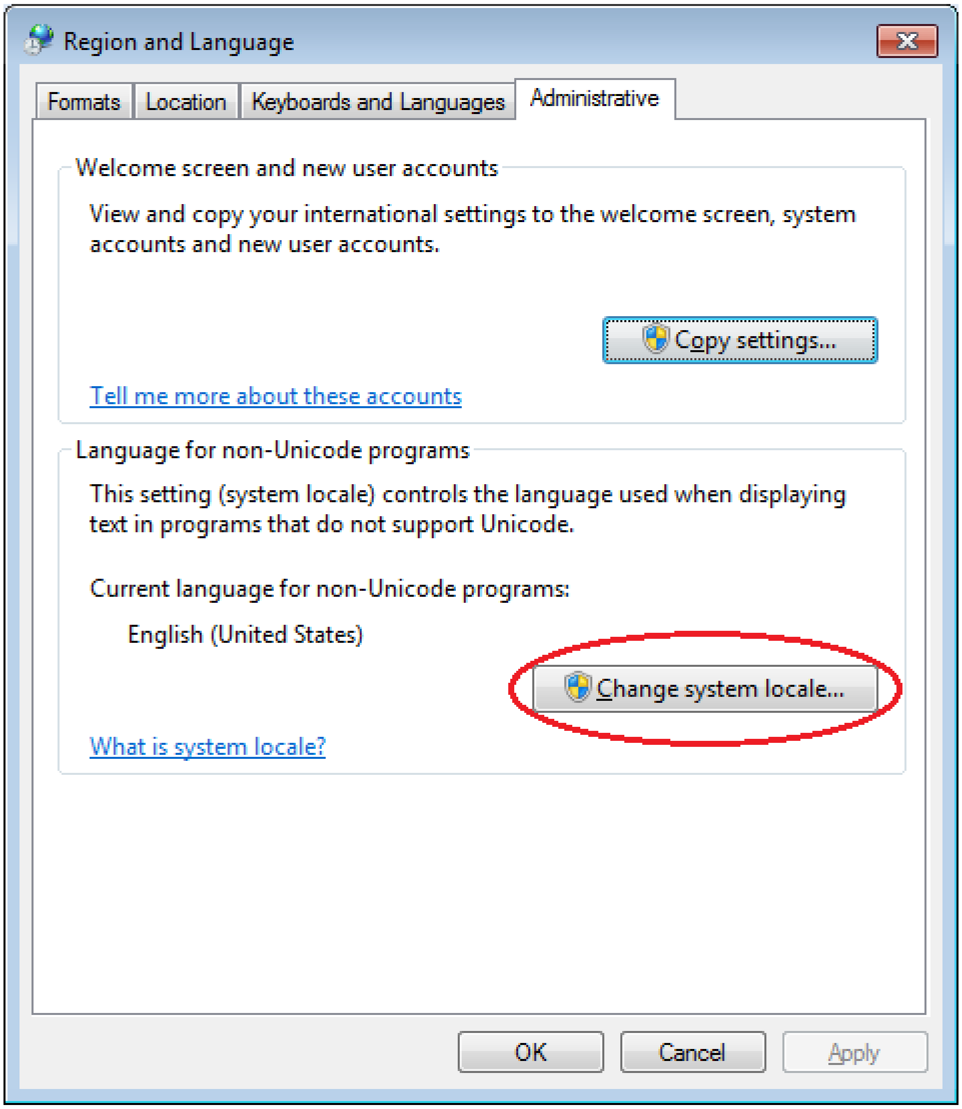
- Because the SCT database used by the reporting system is specified during the ADX installation, you must create it **before** you install the ADX software. The database does not need to contain configuration information, but it must contain a Site object. The SCT database can be a restored backup generated on a different system or an empty database created through SCT.
- The computer that hosts Metasys Advanced Reporting System **must be** a server-class operating system and **must have** a supported SQL Server software version installed. The Metasys Advanced Reporting System is not supported on a computer with SQL Server Express software.
- After the ADX software is installed, you can **replace** the SCT database with a different database, but you must use the **same** archive name. Refer to the *ADS/ADX Commissioning Guide (LIT-1201645)* for details. To rename the database referenced by the reporting system, make the database changes, uninstall the ADX software, and reinstall the ADX software, pointing to the new database.
- If you have a unified ADX, the SCT **must be** installed on the ADX computer that has the Metasys Advanced Reporting system. The local SCT database provides the All Items and user view trees for the reporting system.
- If you have a unified ADX, you must install SQL Server software with Database Services and Reporting Services on the ADX computer.
- If you have a split ADX, you must install Database Engine Services of SQL Server software on the database server computer and Reporting Services of SQL Server software on the web/ application server computer. You must have the appropriate SQL Server software licensing to perform installation on multiple computers. Refer to the *ADS/ADX Commissioning Guide (LIT-1201645)* for licensing information.
- If you have a split ADX, the SCT computer can have any SQL Server or SQL Server Express software installed that is supported by the Metasys software.
- If you have a split ADX, you must perform specific configuration procedures after installing SQL Server software. Refer to the *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
- You cannot add the Metasys Advanced Reporting System during an upgrade if it wasn't configured and installed during the initial installation of the ADX. Ensure you follow all steps included in the installation documentation when configuring the SQL Server software and the initial installation of ADX. During an upgrade installation, if you are not prompted to configure the Reporting feature, you must uninstall the ADX, verify the SQL Server software configuration, and then install the ADX.

Installing Metasys Server for a Non-English Locale

If you are installing the Metasys server software on a computer that is running a non-English Locale, follow the steps outlined here **before** you start the installation.

1. In Control Panel, click **Clock, Language, and Region**.
2. Click **Region** (or **Region and Language**). The Region and Language window appears.
3. Click the **Administrative** tab.

Figure 26: Changing System Locale



Welcome screen and new user accounts

View and copy your international settings to the welcome screen, system accounts and new user accounts.

Language for non-Unicode programs

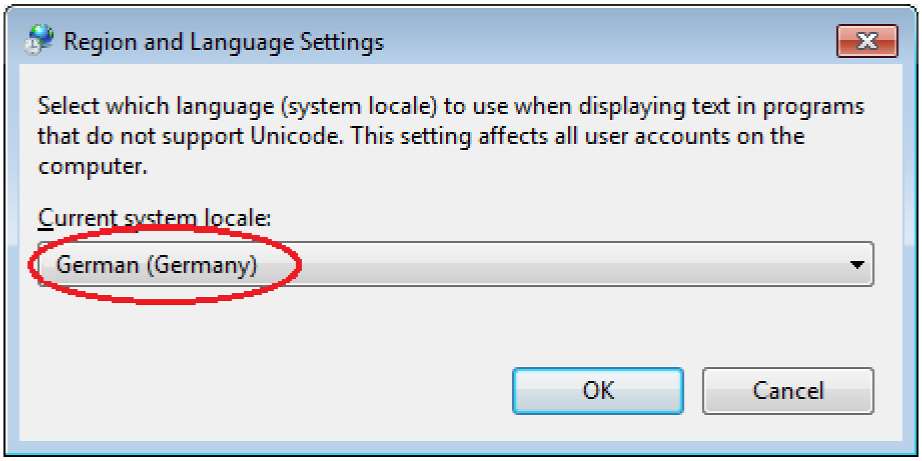
This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.

Current language for non-Unicode programs:

English (United States)

4. In the Language for non-Unicode programs section, click **Change system locale**. Click **Yes** if prompted for consent. The screen for selecting the system locale appears.

Figure 27: Selecting Current System Locale (German Language Example)


Region and Language Settings

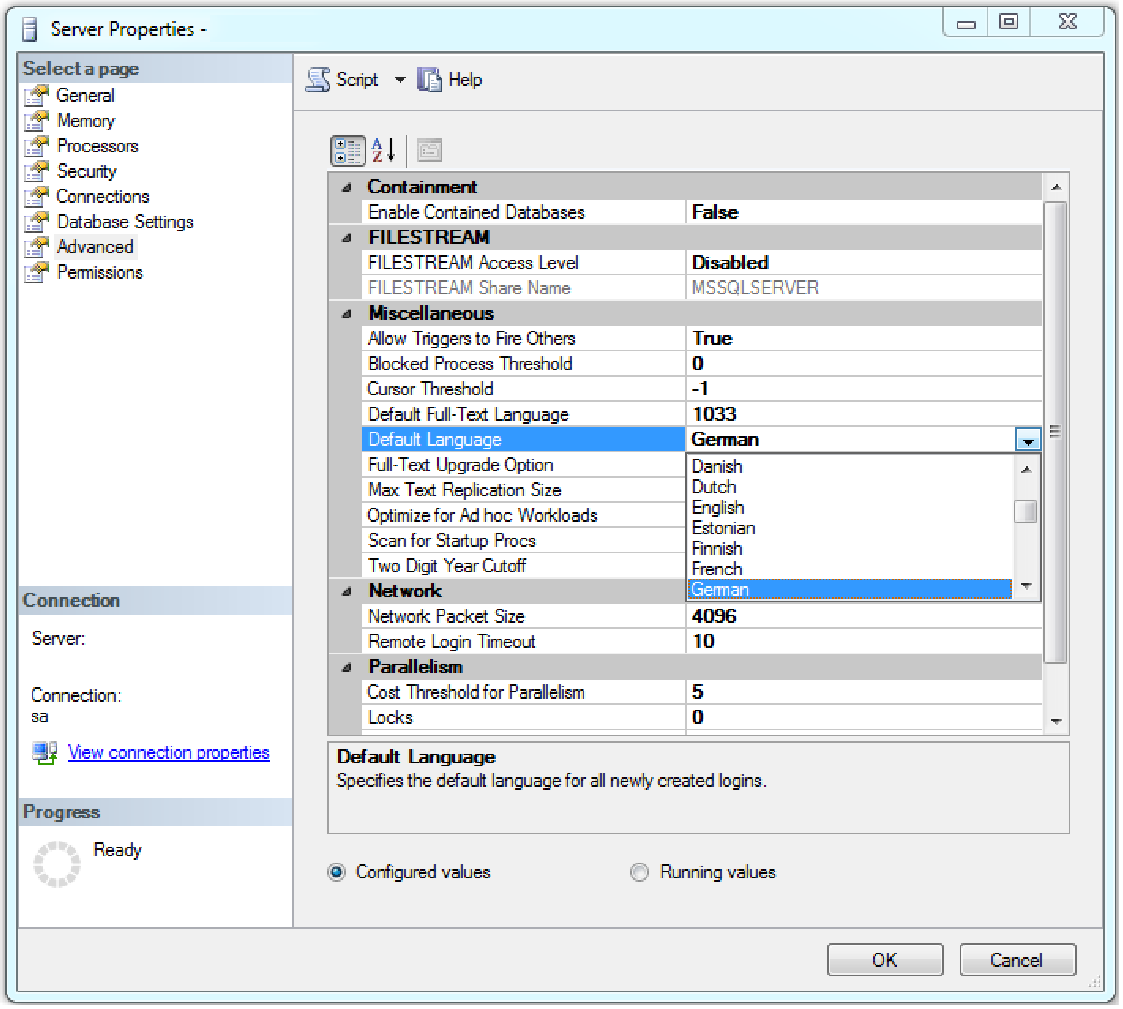
Select which language (system locale) to use when displaying text in programs that do not support Unicode. This setting affects all user accounts on the computer.

Current system locale:

German (Germany)

5. Select the desired language from the drop-down list. Click **OK**, then restart the computer for the changes to take effect.
6. Install a supported edition of SQL Server software. For details, refer to the *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
7. Set the default language of SQL Server to match the locale set on the operating system as follows: Open SQL Server Management Studio and right-click the server instance name in Object Explorer. Click **Properties**. The Properties window appears.
8. Click **Advanced** and set the Default Language property to the language you need. This example shows German. For more details, click here to read a Microsoft article about local language versions of SQL Server.

Figure 28: Setting Default Language on SQL Server



Containment	
Enable Contained Databases	False
FILESTREAM	
FILESTREAM Access Level	Disabled
FILESTREAM Share Name	MSSQLSERVER
Miscellaneous	
Allow Triggers to Fire Others	True
Blocked Process Threshold	0
Cursor Threshold	-1
Default Full-Text Language	1033
Default Language	German
Full-Text Upgrade Option	
Max Text Replication Size	
Optimize for Ad hoc Workloads	
Scan for Startup Procs	
Two Digit Year Cutoff	
Network	
Network Packet Size	4096
Remote Login Timeout	10
Parallelism	
Cost Threshold for Parallelism	5
Locks	0

Default Language
Specifies the default language for all newly created logins.

● Configured values ○ Running values

9. Click **OK** and exit SQL Server Management Studio.

10. After you install the Metasys Server software, use the Language Installation Program (LIP) to set the language on *Metasys* software. Refer to the *Language Installation Program Help (LIT-12011349)*.

Customizing Windows IIS for Metasys API

The Metasys Application Programming Interface (API) enables reading, writing, and commanding of one or more Metasys objects and properties to provide a secure way to bi-directionally integrate with third-party applications. Data is securely extracted from the Metasys system and integrated with third-party data visualization tools to meet robust data analysis and reporting needs.

To ensure the best performance, follow the steps in this section to manually set the rate limit under Internet Information Services (IIS) component of the Metasys Server. Of course, setting a rate limit that is optimized for each system is tricky and may require more than one adjustment. To decide on the best number, you need to consider the types of API calls, frequency of these calls, computer hardware performance, and current system load. For example, because of the amount of data retrieved, calls for historical data are much more taxing on the server than reading attribute values. The best course of action is to follow these instructions and adjust the number of API requests to a value that the system tolerates.

As a prerequisite, follow these steps to enable Rate Limiting on the Metasys Server:

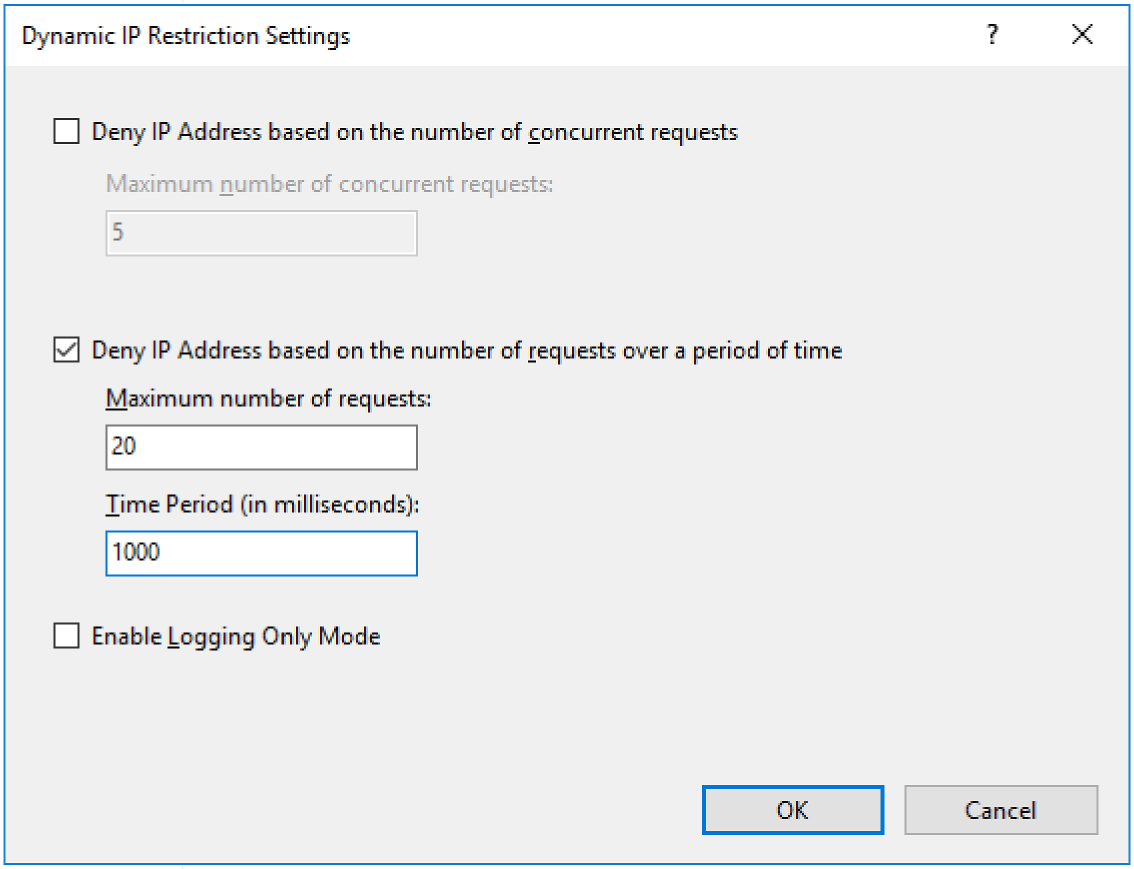
1. In Control Panel, click **Programs** > **Programs and Features**.
2. In the left pane, click **Turn Windows features on or off**.
3. Click **Add roles and features**, then click **Next** twice.
4. Expand **Web Server (IIS)** > **Web Server** > **Security**. Locate a component called **IP and Domain Restrictions**.
5. Select **IP and Domain Restrictions**and complete the Roles and Features Wizard.

Follow these steps to set the Rate Limit in IIS:

1. In Control Panel, click **System and Security** > **Administrative Tools**.
2. Under Administrative Tools, double-click **Internet Information Services (IIS) Manager**.
3. In the left pane, expand the folders to locate Metasys Rate Limit under **Sites**.
4. Select Metasys Rate Limit, and double-click the **IP Address and Domain Restrictions** module in the middle pane.
5. Click on **Edit Dynamic Restriction Settings**.
6. Verify the following settings:

    - **Deny IP Address based on the number of concurrent requests**: not checked
    - **Deny IP Address based on the number of requests over a period of time**: checked
    - **Maximum numbers of requests** = 20
    - **Time Period (in milliseconds)** = 1000
    - **Enable Logging Only Mode**: not checked

Figure 29: Dynamic IP Restriction Settings


Dynamic IP Restriction Settings

□ Deny IP Address based on the number of concurrent requests

Maximum number of concurrent requests: 5

☑ Deny IP Address based on the number of requests over a period of time

Maximum number of requests: 20

Time Period (in milliseconds): 1000

□ Enable Logging Only Mode

7. Click **OK** to save the settings.
8. Restart the computer to ensure the changes are applied.

The values recommended here apply to a high-end system. Lower the maximum number of concurrent requests for a small server to 1 or 2 requests per 1000 ms. If the values you specify are not optimized, the following behaviors can occur:

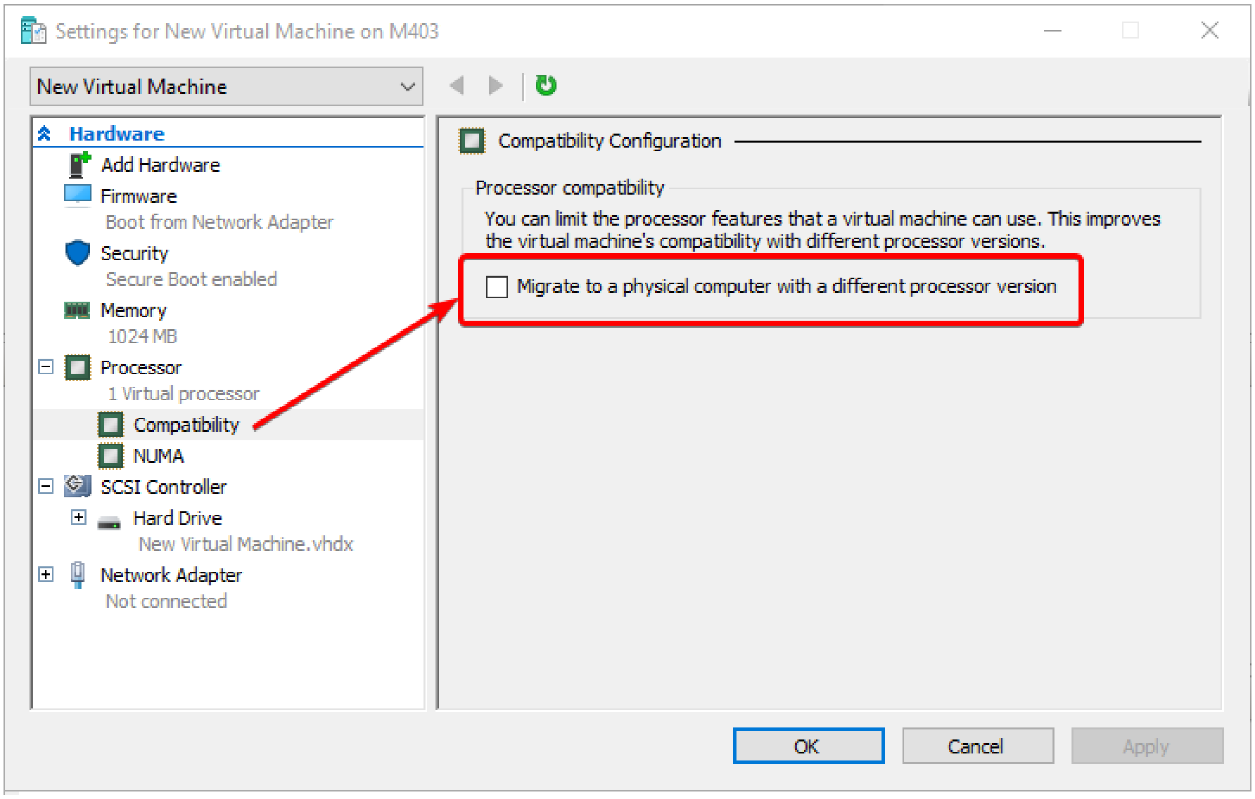
- If the Rate Limit is set to high, the system can slow down or crash before the Rate Limit is reached. Select the **Deny IP Address based on the number of concurrent requests** option and specify 1 or 2 for the maximum number of concurrent requests.
- If the Rate Limit it set to low, an HTTP 429 error or other similar HTTP error can occur. In that case, increase the number of requests incrementally until system performance is satisfactory.

Configuring Virtual Machine for Metasys Server

If you are installing the Metasys Server software on a virtual machine (VM), verify the following **before** you start to install Metasys:

- Ensure that the virtual machine is running in static memory mode, **not** dynamic. Otherwise, operational issues with SQL Server may occur.
- If you are upgrading from a hardware server to a VM, configure the Metasys Server VM with the same amount of memory as the hardware server, or with at least 8 GB of memory.
- Verify that the **Process compatibility**option under **Virtual Machine Settings**> **Processor** > **Compatibility** in Microsoft Hyper-V is **not** selected (Figure 30). For some Intel CPUs, this box is selected by default.

Figure 30: Processor compatibility setting on Metasys Server



Settings for New Virtual Machine on M403

New Virtual Machine

Compatibility Configuration

Processor compatibility

You can limit the processor features that a virtual machine can use. This improves the virtual machine's compatibility with different processor versions.

☐ Migrate to a physical computer with a different processor version

Appendix: General Information and Troubleshooting

Use this appendix for general information and as a troubleshooting reference when installing and upgrading Metasys system software. If you suspect your problem is related specifically to the Metasys Advanced Reporting System, see Appendix: Metasys Advanced Reporting System Troubleshooting. This topic contains the following sections:

- Required Windows operating system roles and features
- Metasys Server Upgrade Plan
- Using MetasysSysAgent User Name and Password
- General Troubleshooting
- Metasys Server Log
- Related Documentation

Required Windows operating system roles and features

The Metasys server software installer enables several roles and features in the Windows operating system for you during the installation process, but does **not** enable all required components. These components are necessary for running the Metasys server. Therefore, it is imperative for you to use this section to validate all required components are set **before** you start the Metasys Server installation. Use the tables below to verify that these components are enabled and active on the computer on which you intend to run the Metasys server. Refer to the table that matches your operating system:

- Windows 10: see Table 51
- Windows 8.1: see Table 52
- Windows Server 2019 or Windows Server 2016: see Table 53

Table 51: Windows 10 roles and features configuration

Category to select	Options to select
Internet Information Services	Web Management Tools • IIS 6 Management Compatibility - IIS 6 Scripting Tools - IIS 6 WMI Compatibility - IIS Metabase and IIS 6 configuration compatibility • IIS Management Console • IIS Management Scripts and Tools World Wide Web Services • Application Development Features - .NET Extensibility 3.5 - .NET Extensibility 4.7 - Application Initialization - ASP.NET 3.5 - ASP.NET 4.7 - ISAPI Extensions - ISAPI Filters • Common HTTP Features - Default Document - Directory Browsing - HTTP Errors - Static Content • Health and Diagnostics - HTTP Logging - Request Monitor • Performance Features - Static Content Compression • Security - IP Security - Request Filtering - Windows Authentication
.NET Framework 3.5 (includes .NET 2.0 and 3.0)	Windows Communication Foundation HTTP Activation

Table 51: Windows 10 roles and features configuration

Category to select	Options to select
.NET Framework 4.7 Advanced Services	• ASP.NET 4.7 • WCF Services - HTTP Activation - Message Queuing (MSMQ) Activation - Named Pipe Activation - TCP Activation - TCP Port Sharing
Microsoft Message Queue (MSMQ) Server	Microsoft Message Queue (MSMQ) Server Core
Windows Powershell 5.1	Windows Powershell 5.1 Engine
Windows Process Activation Service	• .NET Environment • Configuration APIs • Process Model

Table 52: Windows 8.1 roles and features configuration

Category to select	Options to select
Internet Information Services	Web Management Tools • IIS 6 Management Compatibility - IIS 6 Scripting Tools - IIS 6 WMI Compatibility - IIS Metabase and IIS 6 configuration compatibility • IIS Management Console • IIS Management Scripts and Tools World Wide Web Services • Application Development Features - .NET Extensibility 3.5 - .NET Extensibility 4.5 - Application Initialization - ASP.NET 3.5 - ASP.NET 4.5 - ISAPI Extensions - ISAPI Filters • Common HTTP Features - Default Document - Directory Browsing - HTTP Errors - Static Content • Health and Diagnostics - HTTP Logging - Request Monitor • Performance Features - Static Content Compression • Security - Request Filtering - Windows Authentication
.NET Framework 3.5 (Includes .NET 2.0 and 3.0)	Windows Communication Foundation HTTP Activation

Table 52: Windows 8.1 roles and features configuration

Category to select	Options to select
.NET Framework 4.5 Advanced Services	• ASP.NET 4.5 • WCF Services - HTTP Activation - Message Queuing (MSMQ) Activation - Named Pipe Activation - TCP Activation - TCP Port Sharing
Microsoft Message Queue (MSMQ) Server	Microsoft Message Queue (MSMQ) Server Core
Simple Network Management Protocol (SNMP)	WMI SNMP Provider
Windows Powershell 4.0	Windows Powershell 4.0 Engine
Windows Process Activation Service	• .NET Environment • Configuration APIs • Process Model

Table 53: Windows Server 2019 or Windows Server 2016 roles and features configuration

Category to select	Options to select
Web Server (IIS) > Common HTTP Features	• Default Document • Directory Browsing • HTTP Errors • Static Content
Web Server (IIS) > Health and Diagnostics	• HTTP Logging • Request Monitor
Web Server (IIS) > Performance	Static Content Compression
Web Server (IIS) > Security	• Request Filtering • Windows Authentication
Web Server (IIS) > Application Development	• .NET Extensibility 3.5 • .NET Extensibility 4.6 • Application Initialization • ASP.NET 3.5 • ASP.NET 4.6 • ISAPI Extensions • ISAPI Filters

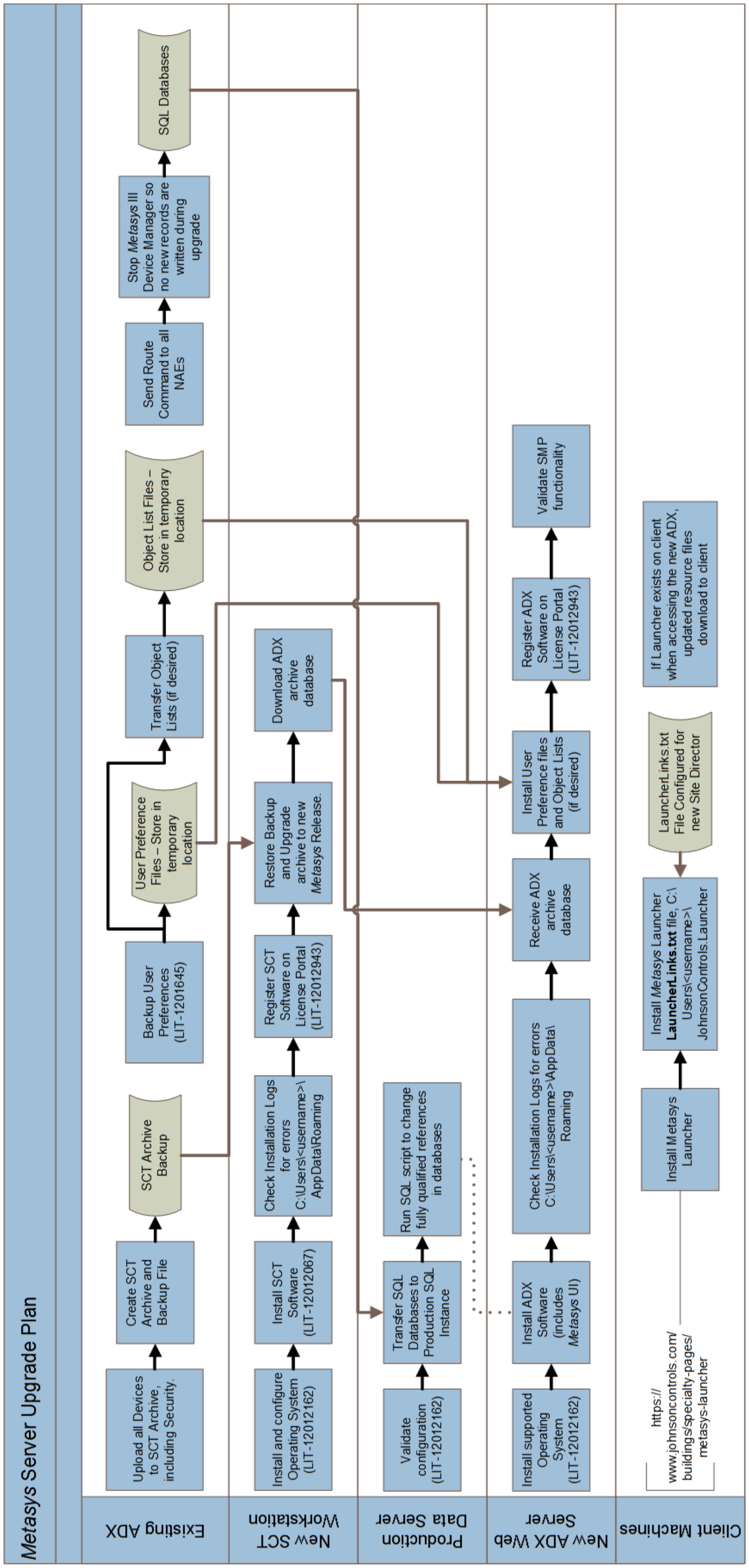
Table 53: Windows Server 2019 or Windows Server 2016 roles and features configuration

Category to select	Options to select
Management Tools	• IIS 6 Management Console • IIS 6 Management Compatibility - IIS 6 Metabase Compatibility - IIS 6 Scripting Tools - IIS 6 WMI Compatibility • IIS Management Scripts and Tools
.NET Framework 3.5 Features	• .NET Framework 3.5 • HTTP Activation
.NET Framework 4.6 Features	• .NET Framework 4.6 • ASP.NET 4.6 • WCF Services - HTTP Activation - Message Queuing (MSMQ) Activation - Named Pipe Activation - TCP Activation - TCP Port Sharing
Message Queuing	• Message Queuing Services - Message Queuing Server
Remote Server Administration Tools	• Feature Administration Tools - SMTP Server Tools - SNMP Tools
SNMP Server	SNMP WMI Provider
Windows Powershell	• Windows Powershell 5.1 • Windows Powershell 2.0 Engine • Windows Powershell ISE
Windows Process Activation Service	• Process Model • .NET Environment 3.5 • Configuration APIs
WoW 64 Support	n/a

Metasys Server Upgrade Plan

The following flowchart summarizes the upgrade plan that applies to most system installations. Use this diagram as a guide when performing a Metasys system upgrade.

Figure 31: Metasys Server Upgrade Plan


Metasys Server Upgrade Plan
Existing ADX
New SCT Workstation
Production Data Server
New ADX Web Server
Client Machines
Upload all Devices to SCT Archive, including Security.
Create SCT Archive and Backup File
SCT Archive Backup
Backup User Preferences (LIT-1201645)
User Preference Files – Store in temporary location
Transfer Object Lists (if desired)
Object List Files – Store in temporary location
Send Route Command to all NAEs
Stop Metasys III Device Manager so no new records are written during upgrade
SQL Databases
Install and configure Operating System (LIT-12012162)
Install SCT Software (LIT-12012067)
Check Installation Logs for errors C:\Users\<username>\AppData\Roaming
Register SCT Software on License Portal (LIT-12012943)
Restore Backup and Upgrade archive to new Metasys Release.
Download ADX archive database
Validate configuration (LIT-12012162)
Transfer SQL Databases to Production SQL Instance
Run SQL script to change fully qualified references in databases
Install supported Operating System (LIT-12012162)
Install ADX Software (includes Metasys UI)
Check Installation Logs for errors C:\Users\<username>\AppData\Roaming
Receive ADX archive database
Install User Preference files and Object Lists (if desired)
Register ADX Software on License Portal (LIT-12012943)
Validate SMP functionality
https://www.johnsoncontrols.com/buildings/specialty-pages/metasys-launcher
Install Metasys Launcher
Install Metasys Launcher LauncherLinks.txt file, C:\Users\<username>\JohnsonControls.Launcher
LauncherLinks.txt File Configured for new Site Director
If Launcher exists on client when accessing the new ADX, updated resource files download to client

Notes:
BLACK lines: task workflow / BROWN lines: file transfer
Drive letter must match the actual path of *Metasys* databases in SQL Server. Map network drive example: \\165.134.228.52\C$ would map the local web server C:\ drive as the same drive letter as the SQL Server database drive. The install program checks this drive for space during the install.

Using MetasysSysAgent User Name and Password

The Security Administrator system provides one predefined standard administrator on the Metasys Server called MetasysSysAgent. For the password of this user, contact your local Johnson Controls representative.

For security purposes, you must change the default MetasysSysAgent account password when you log on the system for the first time. Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)* for more details about the predefined administrator.

Note the following:

- All passwords are case sensitive and must meet complexity requirements. Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.
- The Johnson Controls license agreement appears the first time you log in. You must accept the terms of the license before continuing.
- Your MetasysSysAgent password does not need to match the password you use to log into your computer.
- The Basic Access account (BasicSysAgent) that came with Release 10.1 and earlier is no longer available. If you are upgrading to Release 11.0, the BasicSysAgent account is converted to a standard access user account.

General Troubleshooting

See Table 54 for general troubleshooting information. If you are troubleshooting an ADX with Metasys Advanced Reporting System, see *Metasys Advanced Reporting System Troubleshooting*.

Table 54: Troubleshooting

Problem	Solution
You experience installation problems and would like to consult the error log.	The error messages are located in the following folder: `C:\Users\<username>\AppData\Local` Metasys_Server_x.x_<date>.html, where x.x is replaced by the release version number.
During installation, you see the following error message: `Install complete, but exceptions during historian database upgrade.`	Before you restart the computer, use the Metasys Post Install (MPI) Database tool to complete necessary data type conversion work. Refer to the *Database Tools Commissioning Guide (LIT-12012254)*.
During ADS/ADX installation, a RabbitMQ command prompt window opens that contains the following error text: `Error: {:enabled_plugins_mismatch, 'c:\\Users\\ADMINI~1\\AppData\\Roaming\\RabbitMQ\\ENABLE~1', 'c:\\PROGRA~3\\JOHNSO~1\\RabbitMQ\\ENABLE~1'}.`	The computer has two instances of the RabbitMQ database. To resolve, open a Command prompt as Administrator and run the **Enable_RabbitMQ_Management.bat** script that is located in the following location on the ADS/ADX server: C:\ProgramData\Johnson Controls\MetasysIII\Diagnostics\Utilities

Table 54: Troubleshooting

Problem	Solution
During an ADX upgrade, you see the following error: `ERROR - There was an error setting up the JCIHistorianDB Database for Advanced Reporting; Timeout expired.`	The JCIHistorianDB upgrade script timed out during ADX installation. Ordinarily, this script completes within a few seconds, but it may take longer if the existing JCIHistorianDB is very large or the server is busy with other activities. If this timeout occurs during ADX installation, uninstall the ADX, restart, wait 5 to 10 minutes, and then reinstall ADX.
After a successful ADS/X upgrade, you see the following content under the View Status option: `* Device Upgrade: Password changed for the following users.... <list of user names>`	The device upgrade process lists the user names whose passwords were updated to the default password that you specified when you performed the upgrade. Each user enters this default password upon initial log in, then defines a new password when prompted.
During an ADS/ADX installation or upgrade, you see the following error: `Could not determine SqlServer instance name.`	This problem can occur if the computer has a previous release of Metasys UI software installed. Uninstall Metasys UI and try the installation or upgrade again.

Table 54: Troubleshooting

Problem	Solution

After an ADS/ADX upgrade, you see one of the following errors:
`Server is currently busy and data refresh will be delayed.`
`Unable to connect to server.`
	This problem occurs when the frameworkproperties.properties file does not update correctly. This file contains network parameters for ADS/ADX or ADS-Lite communication.
	To solve this problem:
	1. Using Windows Explorer, browse to `C:\Inetpub\wwwroot\Metasysiii\UI\Com\JCI\Framework`.
	2. Open the frameworkproperties.properties file in a text editor.
	3. Find the following parameters and make sure the values are correct for your ADS/ADX or ADS-Lite:
	For ADS or ADS-Lite:
	`readAlarms=9`
	`remoteDispatcherPool.size.defaultPool=3`
	`remoteDispatcherPool.size.cpm=2`
	For ADX:
	`readAlarms=4`
	`remoteDispatcherPool.size.defaultPool=0`
	`remoteDispatcherPool.size.cpm=0`
	4. Save and close the file.
	ⓘ **Note:** Do not change any other parameters. Also, do not change the parameters above to values other than those noted in this solution.

After an upgrade, one or more of the following happens: - The NAE serial printer DDA does not function correctly - A Metasys Reporting System refresh does not occur as expected - The Action Queue does not behave as expected - A behavior controlled by a .config file does not happen as expected	This problem occurs because upgrades overwrite the .config files for the Metasys system. To retain custom settings related to the serial printer DDA, Metasys Advanced Reporting System refresh rate, and other system behavior, you must restore these customizations after each upgrade. Refer to the *ADS/ADX Commissioning Guide (LIT-1201645).*

Table 54: Troubleshooting

Problem	Solution
After an ADS/ADX upgrade, you see one of the following errors: `The local event repository is getting full. Acknowledge or Discard some events to free up some space.`	The event buffer of the network engine is almost full and the ADS/ADX cannot clear out the events. This issue may occur after the ADS/ADX is upgraded to new release but the network engine remains at an older release. To resolve, manually delete all the events from the network engine.
After an ADS/ADX upgrade, Spaces or the Network tree do not appear when you log on the Metasys UI.	Allow one to two hours per 500 engines for the Online Archive to gather and populate the attributes and other data displayed in the Building Network tree. We recommend not accessing the Building Network tree objects and viewing the object's Detail widget during the initial startup and sync. Furthermore, do not issue Bulk Commands through the Advanced Search feature in the Metasys UI during initial startup and sync.

During an ADS/ADX install or upgrade, one of the following errors appears on the screen for the Reporting tab:
`Error connecting to database. Could not find server or credentials are invalid.`
`Archive database could not be found in server instance.`
	For the first error, the specified user credentials are incorrect or the syntax used to specify the server name in the Server Name field is incorrect. The correct syntax is: **<servername>** (default instance) or **<servername>\<database instance>** (named instance). Valid examples:
	localhost
	10.10.9.50
	10.10.9.50\MySQLInstance
	For the second error, the archive name specified in the SCT Archive field is incorrect.

Table 54: Troubleshooting

Problem	Solution
During an ADS/ADX upgrade, the following messages appear: If you proceed with the upgrade process, the following Metasys users will be locked out and will not be able to login until their password is reset by an Administrator: FipsLockUsers.txt To prevent user lock out, cancel the upgrade process, then remove the Never Expire property and set a new password for the affected users. The following users are affected: - Release 7.x or earlier sites: All users. - Release 8.0 and later sites: Users with passwords that have not been changed since the upgrade.	As the result of FIPS 140-2 compliance at Metasys Release 11.0, existing user accounts are affected. Cancel the upgrade process. Then, for each affected user, set a new password and verify that the Never Expire property under Account Policy is not set. The FipsLockUsers.txt file lists the user accounts that you need to fix. Additionally, for all other Metasys users, set a new password for any user who has not changed their password in more than two years. Then, restart the upgrade process.
During an ADS/ADX install or upgrade, the following message appears: Unsupported SQL Server version <version number>. Update to a supported SQL version and its latest Service Pack and Cumulative Update.	The version of SQL Server currently installed is not compatible with the ADS/ADX at Release 11.0. Exit the installer and see Prerequisite Software Checklist for Installation and Upgrade for a list of supported versions of SQL Server.
During an ADS/ADX install or upgrade, the following message appears: We recommend that you check for updates to the SQL Server software. If applicable, apply the latest service pack and cumulative update.	This message is simply a notification that the version of SQL Server software currently installed on the computer is at the minimum level required for that version. The message is not prompting you to upgrade the SQL Server software that is currently installed on the computer. Click OK to continue with the installation, or click Cancel if you want to stop and upgrade to a later, supported version of SQL Server.

Table 54: Troubleshooting

Problem	Solution

An update error occurs when you are trying to install the ADX software on a split ADX system.	A change from Microsoft made the Allow Updates server configuration option obsolete, adversely affecting the installation of ADX software. You need to execute a SQL Server script on the database server computer for a split ADX installation to work. Follow these steps:
	1. Start SQL Server Management Studio on the database server computer.
	2. Click **New Query**, and execute the following query:
	`exec sp_configure 'show advanced options', 1;`
	`GO`
	`RECONFIGURE WITH OVERRIDE;`
	`GO`
	`sp_configure 'allow updates', 0;`
	`GO`
	`RECONFIGURE WITH OVERRIDE;`
	`GO`
	3. Run the ADX software installation again on the web/application server computer.

This error message appears while uninstalling prior releases of ADS/ADX software:
`Exception= -2147217900`
`User 'g3-user' does not exist in the current database.`
`Last command=exec sp_dropuser N'g3-user'`
	The ADS/ADX uninstallation program could not locate and drop user **g3-user**. This situation does not affect the uninstallation. You can ignore the message. The ADS/ADX uninstallation should complete normally.

When you uninstall the ADX with Metasys Advanced Reporting, you receive the following error message: `ADX uninstall could not remove the folder C:\inetpub\wwwroot\MetasysReports. You should remove the Folder(s) and all contents manually.`	When this error occurs, the uninstall program could not remove the MetasysReports folder. Click **OK** to continue. After uninstalling the ADX software, manually delete the following folder and all its contents: `C:\inetpub\wwwroot\MetasysReports`

Table 54: Troubleshooting

Problem	Solution
When you uninstall the ADS/ADX, you receive the following error message: `FIPS Update installation detected. Please remove FIPS Update and then run this setup again.`	When this error occurs, the uninstall program could not remove the ADS/ADX software because the Metasys FIPS component must be uninstalled from the computer. Remove the **FIPS License Update** first, (Uninstalling and unlicensing FIPS component), then remove the ADS/ADX software.
You cannot browse from a client computer into the SMP UI or SCT UI on the ADS, ADS-Lite, or ADX.	The computer's firewall settings may be set incorrectly. See Configuring the Windows firewall for steps on how to configure the firewall.
During the installation of Windows operating system features, a Windows Features dialog box appears that reads: `Windows needs files from Windows Update to finish installing some features.` Two choices are given: • Download files from Windows Update • Don't connect to Windows Update	Windows is trying unsuccessfully to access the Internet to retrieve .NET Framework 3.5 files or other necessary updates. Select either choice and refer to the Windows support website for further instructions.
When you try to navigate to a website using a server-class operating system with the Enhanced Security Configuration enabled, the Internet Explorer web browser displays a message box saying the content is blocked.	Add the site to your web browser as a trusted site or disable Enhanced Security. To disable Enhanced Security for the server operating system, follow these steps: 1. Start Server Manager. 2. On the Server Manager window, click **Local Server**. 3. In the right column, set the parameter IE Enhanced Security Configuration to **Off**.

Table 54: Troubleshooting

Problem	Solution
The Metasys III Device Manager and Metasys III Action Queue services stop every time the services are started. The ADS/ADX is not functional. The Site Management Portal generates this error message: `Unable to Login. Unexpected Error.`	The Windows server computer `(web/application server computer in a split configuration)` must allow the Metasys III Device Manager and Metasys Action Queue services to run. The services may need to be explicitly allowed to run. Use the Security Configuration Wizard to identify the Metasys III Device Manager service and Metasys III Action Queue service as Windows services that are allowed to run.
	This error may appear when a user is denied access to the ADS/ADX computer over the network. To resolve this problem: 1. Select ***Control Panel*** > ***System and Security*** > ***Administrative Tools*** > ***Local Security Policy*** > ***Local Policies*** > ***User Rights Assignment***. 2. With User Rights Assignment selected in the left pane, right-click **Deny access to this computer from the network** in the right pane, then select Properties. 3. On the Local Security Settings tab, make sure that the user's name is not listed. If the user’s name appears, select it and click **Remove**. 4. Close all windows.
	Anti-spyware software is installed on the computer and is not configured to allow the Metasys III Device Manager Service or Metasys III Action Queue Service to run; or, the anti-spyware software is not allowing the **hosts** file to be updated. Refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)*.

Table 54: Troubleshooting

Problem	Solution
You have a general problem with the SQL Server Software installation or upgrade (including error messages or non-functional tools).	To resolve this problem: 1. Start SQL Server Management Studio and drop all databases that begin with JCI and drop all Reporting Services databases. 2. Remove all SQL Server software related files using Add/Remove Programs. 3. Attempt to install SQL Server software again. **Always restart the computer after each installation.**
	Because SQL Server software versions and configurations vary, your upgrade procedure may differ from what is documented in Johnson Controls literature. If your upgrade does not follow the steps published in our literature and you are unsure about which selections to make, go to http://technet.microsoft.com/en-us/default.aspx for information. Perform a search based on the version of SQL Server software you want to install; for example, **SQL Server 2019** or **Upgrading to SQL Server 2019**.

While using the SQL Installer tool, you receive a user or error message during SQL Server software installation or upgrade. Possible messages include:
`SQL Server Install error`
`Instance Name already installed`
`Install failed - Missing Windows Installer 5.0`
`Install failed - Missing .NET 3.5 SP1`
`No new features were installed during the setup execution`
`The OS does not meet the minimum requirements for this SQL Server install`
`Install failed - Bad software key`
`WARNING: Please install the following prerequisites: .NET 3.5 SP1, Windows Installer 5.0`
	Consult the error log file. The error messages file is located in the following folder:
	`C:\Program Files\Microsoft SQL Server \<number` based on the SQL release>\Setup Bootstrap\Log\Summary.txt
	Correct the problem and try the SQL Server installation or upgrade again.

Table 54: Troubleshooting

Problem	Solution
While using the SQL Installer tool, you experience installation problems after you edit the text in the Command Line Options window of the SQL Installer.	The text within the Command Line Options window contains errors. Correct the errors or restart the SQL Installer so that the Command Line Options window defaults to its original content.
You are trying to upgrade a split ADX but do not know the SQL Server database instance name in use by the ADX.	Log in to the database server of the split ADX. Start the Registry Editor (regedit). In the tree on the left, browse to **HKEY_LOCAL_MACHINE\SOFTWARE \Johnson Controls\Metasys\ADS**. The DBServer field displays the name of the SQL Server instance currently in use by the ADX.
The ADS/ADX installation or upgrade fails and the following error message appears: `Violation of PRIMARY KEY constraint error.`	In the Control Panel, open the System Properties window and verify that the Verify that the computer name meets the following criteria: • begins with a letter, not a number • contains a maximum of 15 characters • contains only letters A–Z (upper or lower case), numbers 0–9, and hyphens • does not end in ADS • matches the object ID of the device object as defined in the SCT archive database (upgrade only) If the computer name does not meet this criterion, change the computer name. Refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*.
During installation of SQL Server Management Studio, you receive this error message: `Setup is missing prerequisites - MSXML6`	You need to install Microsoft .NET Framework 3.5 before you install Microsoft SQL Server Management Studio software. Cancel the installation and install .NET Framework 3.5 first, then install SQL Server Management Studio software.
During SNE or SNC commissioning, you find that you cannot change the JCI IP Address and Computer Name attributes at the same time.	For SNE and SNC engines upgraded to Release 11.0, you cannot change the Computer Name and JCI IP Address at the same time. If you need to change both of these attributes, change one at a time. The engine resets after each operation.

Table 54: Troubleshooting

Problem	Solution
The ADS/ADX software does not function correctly after you do one of the following: • Attempt to reinstall SQL Server software because it appears to be damaged. • Upgrade from an older version of SQL Server Express software to a newer version of SQL Server Express software outside the regular upgrade process.	To correctly change your SQL Server software outside the usual install or upgrade process, follow these steps: 1. Back up all archive databases and back up the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 2. Uninstall the SCT and ADS/ADX software using Add/Remove Programs or Uninstall a Program. 3. Reinstall or upgrade SQL Server software as you intended. 4. Restore the archive databases and the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 5. Reinstall the ADS/ADX. If you have already changed SQL Server software without uninstalling the ADS/ADX, follow these steps: 1. Back up all archive databases and back up the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 2. Uninstall the ADS/ADX software using Add/Remove Programs or Uninstall a Program. 3. Restore the archive databases and the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 4. Reinstall the ADS/ADX.

Table 54: Troubleshooting

Problem	Solution
After upgrading to a newer version of SQL Server, ADS/ADX no longer starts.	To correctly change your SQL Server software outside the usual install or upgrade process, follow these steps: 1. Back up all archive databases and back up the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 2. Uninstall the ADS/ADX software. 3. Reinstall or upgrade SQL Server software. 4. Restore the archive databases and the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 5. Reinstall the ADS/ADX. If you have already changed SQL Server software without uninstalling the ADS/ADX, follow these steps: 1. Back up all archive databases and back up the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 2. Uninstall the ADS/ADX software. 3. Uninstall the SQL Server software. 4. Using Windows Explorer, browse to `C:\Inetpub\wwwroot` and delete the **MetasysIII** folder. 5. Browse to `C:\WINDOWS\inf\009` and `C:\WINDOWS\inf\inc` and delete the **MSSQLServer** folder in each one. 6. Install SQL Server software. 7. Restore the archive databases and the historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting. 8. Reinstall the ADS/ADX.

Table 54: Troubleshooting

Problem	Solution
If you back up a database using a newer version of SQL Server software, you cannot restore the database on a system using any older version of SQL Server software.	After you convert databases created with an older version of SQL Server software to a newer version of SQL Server software, you cannot go back to the older format. Two different SQL Server software formats cannot coexist on the same computer. If you have some customers who use the older version of SQL software and some customers who use the newer version of SQL software, you must maintain the SQL software versions on separate computers. You can work around this issue by downloading from a system running a newer version of SQL Server software and then uploading the archive into a system running an older version of SQL Server software.
During an installation or upgrade of SQL Server Express, you may see a reference to a file named sqlncli.msi or the following error message: `An installation package for the product Microsoft SQL Native Client cannot be found.`	To resolve this error: 1. Cancel the installation or upgrade. 2. In Control Panel, go to Add or Remove Programs. 3. Select **Microsoft SQL Server Native Client**. 4. Click **Remove** and follow the instructions. 5. Attempt the installation or upgrade again. You may see slightly different screens during the installation or upgrade after you remove the native client.
The ADS/ADX does not start.	Follow these steps to verify the correct SQL Server software protocols are enabled: 1. Start SQL Server Configuration Manager. 2. Expand SQL Server Network Configuration. 3. Select **Protocols for MSSQLSERVER** (or other instance name). 4. In the list of protocols, make sure Named Pipes and TCP/IP are enabled. If Named Pipes and TCP/IP are not enabled, open each and enable them. 5. Close SQL Server Configuration Manager. 6. Restart your computer.

Table 54: Troubleshooting

Problem	Solution
The following error appears when you try to log in to the ADS/ADX: `Unable to Authorize Active Directory User.`	If this server is running at an MVE site, the Active Directory single sign-on (SSO) feature is not available for the ADX UI (per design). Alternatively, the user account settings for the Active Directory may be invalid. To work around this problem, follow these steps: 1. Log in to the Site Management Portal UI and select ***Tools*** > ***Administrator***. 2. Select ***Server Configuration*** > ***Active Directory***. 3. Select the user in the Active Directory Service Accounts table and click **Edit**. 4. Verify the user name and provide the user's current password. 5. Click **Save**. To permanently solve this problem, use a dedicated Active Directory account that has the password set to never expire as the Active Directory Service Account. (For details, refer to the *Security Administrator System Technical Bulletin [LIT-1201528]*).
The following error appears when you try to log in to the ADS/ADX: `Error: Unable to Login. Unexpected Error.`	**Solution 1:** The Internet Explorer web browser proxy setting is set to bypass the proxy server for local addresses. To resolve this problem, start the browser and select ***Tools*** > ***Internet Options***. Click the **Connections** tab, then LAN Settings. On the Local Area Network Settings window, select **Automatically Detect Settings** and select **Use automatic configuration script**. Type the address of the proxy server. Then, clear both check boxes under the Proxy server section. Relaunch the browser. **Solution 2:** The URL of the ADS/ADX you entered included a space. Remove the space and reload the page. **Solution 3:** The Launcher is configured to use a proxy server, even though the network does not require a proxy server. Open the Launcher and click the **Network Settings** button. On the Network Settings window, select **Use browser settings**. **Solution 4:** Microsoft SQL Server is not running. Start the SQL Server service with the SQL Server Configuration Manager.

Table 54: Troubleshooting

Problem	Solution
(cont.)	**Solution 5:** SQL Server is missing from the computer’s Path variable. To resolve this problem, follow these steps: 1. Select ***Settings*** > ***Control Panel*** > ***System***. 2. Click the **Advanced** tab, then click the **Environment Variables** button. 3. Under System Variables, double-click on the Path entry. 4. On Edit System Variable window, make sure the SQL path is present somewhere within the variable value string. For SQL Server 2019 software, the path should be: `C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL \Binn`. For SQL Server 2016 software, the path should be: `C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL \Binn`. 5. If the path is not present, add it using a semicolon (;) at the start of the string as a separator. **Solution 6:** The computer contains files from an earlier operating system or from an earlier version of Metasys software that is conflicting with the updated software. Verify that a folder with an older OS does not exist on the hard disk (for example, WINDOWS.OLD). **Solution 7:** The computer is using an older version of the Internet Explorer web browser. Upgrade the browser to version 11.

Table 54: Troubleshooting

Problem	Solution
A message box appears displaying the error `Intranet settings are turned off by default` within the Windows Internet Explorer browser window when you try to launch the SMP UI:	To avoid the Intranet Settings Turned Off dialog box, open Windows Internet Explorer and click to clear the **Automatically detect intranet network** check box in ***Tools*** > ***Internet Options*** > ***Security*** > ***Local Intranet*** > ***Sites***. Select the following options: • Include all local (intranet) sites not listed in other zones • Include all sites that bypass the proxy server • Include all network paths (UNCs)
The following error appears when you try to open ADS/ADX from the Launcher: `Missing Resource File.`	You are trying to use an older version of Launcher that is not compatible with this ADS/ADX release. Uninstall the old version of Launcher, then try again. Or to have the latest Launcher pushed to your computer directly from the ADS/ADX computer, open the browser and go to `http://<server computer name or IP address>/launcher.msi`.
The error `Device archive failed (543)` appears when you attempt to upload the ADS into SCT.	Ensure that **English (United States)** is the preferred language in the Windows control panel.

Metasys Server Log

If requested, forward the install log to the Field Support Center for further analysis. The log file is located here:

C:\Users\<username>\AppData\Local

Related Documentation

Table 55: Related Documentation

For Information On	See Document
Using the Metasys Site Management Portal User Interface	*Metasys SMP Help (LIT-1201793)*
Using the SCT User Interface (Including SCT Troubleshooting)	*Metasys SCT Help (LIT-12011964)*
Configuring or Commissioning the ADS	*ADS/ADX Commissioning Guide (LIT-1201645)*
Metasys Database Manager	*Metasys Database Manager Help (LIT-12011202)*
Network and IT Considerations	*Network and IT Guidance Technical Bulletin (LIT-12011279)*
Licensing Metasys Software	*Software Manager Help (LIT-12012389)*
NAE/NIE Update Tool	*NAE/NIE Update Tool Technical Bulletin (LIT-12011524)*
System Security	*Security Administrator System Technical Bulletin (LIT-1201528)*

Table 55: Related Documentation

For Information On	See Document
Metasys Export Utility	*Metasys Export Utility Installation Instructions (LIT-12011527)*
Controller Configuration Tool (CCT)	*CCT Installation Instructions (LIT12011529)*
	Controller Tool Help (LIT-12011147)

Special Scenarios

Use this section for information about special scenarios to consider when installing Metasys Server software, such as customizing the install location and configuring multiple network cards. The appendix contains the following sections:

- Specifying Custom Locations for Metasys Server Application and Databases
- Moving Metasys Historical Databases to a Custom Location
- Configuring Additional Network Cards
- Adding the Metasys Advanced Reporting System to an Existing ADS/ADX
- Changing the Database Referenced by the Metasys Advanced Reporting System

Specifying Custom Locations for Metasys Server Application and Databases

By default, the Metasys Server software is installed on the local disk drive, typically drive C:. Likewise, the installer creates the Metasys system databases using the SQL Server default location, also typically the C: drive. However, by following the steps in the section, you can specify a different disk location of where to install the files and databases (for example, drive E:).

Important: The Metasys Server installation can fail if you specify a drive other than C:\ with a custom path that contains parentheses, or other special characters, in the installation options for Server software. For example, the installation can fail if you specify a path like `D:\Program Files (x86)\Johnson Controls`.

If you accept drive C: as the location for files and databases, skip this section.

In order to install the Metasys Server application to an alternate disk drive location, use the **Custom** installation method. You can also install the application databases in a custom location, but to do so, you need to create the Metasys historical databases **before** you begin the installation by using the SQL Server Management Studio. The Metasys Server setup then detects the presence of the historical databases and installs the databases at that location.

Note: Even if the existing databases were created in a specified location at an earlier release, the JCIReportingDB and SpacesAuthorization databases are created in the SQL Database Properties default location.

The following table indicates the application and database default locations.

Table 56: Default Application and Database Locations

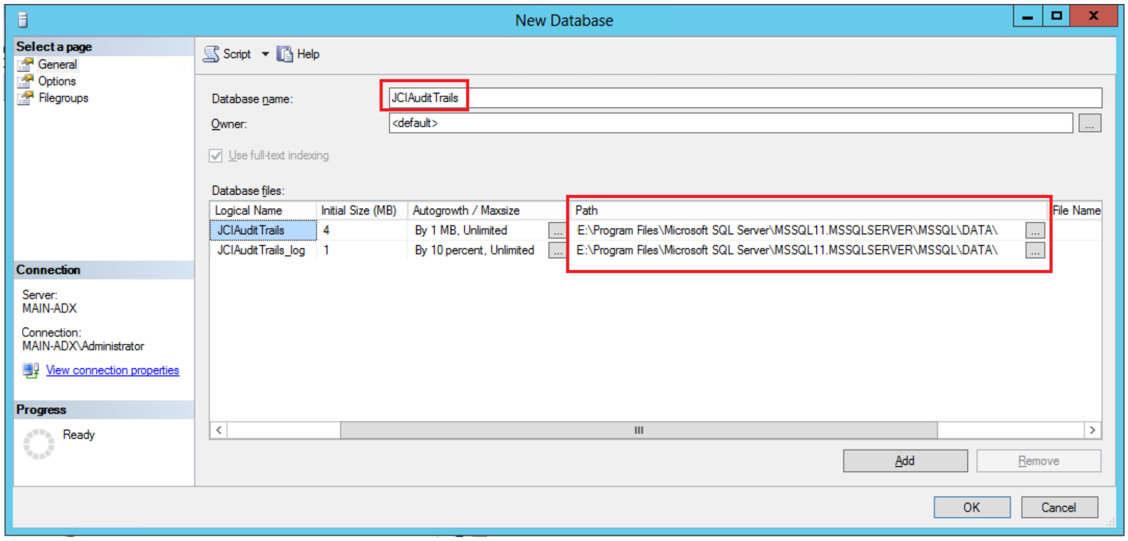
Installed Item	Default Location
Metasys Server Application	C:\Program Files (x86)\Johnson Controls\MetasysIII on a 64-bit system
Metasys System Databases	C:\Program Files\Microsoft SQL Server \MSSQL<version>.MSSQLSERVER\MSSQL\DATA

Follow these steps to create the databases at a custom location. (For more background on changing SQL Server database default locations, browse to this link: https://msdn.microsoft.com/en-us/library/dd206993(v=sql.120).aspx).

1. Install the version of SQL Server software that is recommended for your operating system and supported for Metasys software on the alternate disk drive. You can use the SQL Installer tool to specify a custom install path. For details, see SQL Server Software.
2. If you installed one of the full versions of SQL Server software, skip to the next step. If you installed a version of SQL Server Express, verify if you also have SQL Server Management Studio under the SQL Server program group. If that application is not on the computer, install the SQL Server Management Studio software on the drive that you just installed SQL Server software. For details, refer to the *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
3. Start SQL Server Management Studio. Log in as the SQL Server sa administrator, or with a Windows user account that has administrative rights to SQL Server. The Object Explorer appears.
4. Use Object Explorer to manually create the following system databases on the alternate disk drive one at a time:

   JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIItemAnnotation, JCIReportingDB, SpacesAuthorization, and MetasysReporting
5. When you define the database, assign the Owner as **<default>** and specify a custom location in the Path field. Use the browse button next to each path field to locate where you wish to create the database.

Figure 32: Example of Defining JCIAuditTrails Database



Database name: JCIAuditTrails

Owner: <default>

☑ Use full-text indexing

Server: MAIN-ADX

Connection: MAIN-ADX\Administrator

Database files:

Logical Name	Initial Size (MB)	Autogrowth / Maxsize	Path	File Name
JCIAuditTrails	4	By 1 MB, Unlimited	E:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\	
JCIAuditTrails_log	1	By 10 percent, Unlimited	E:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\	

6. Save the new database.
7. Repeat for each Metasys system database listed in Step 4.
8. Create an empty folder structure for the third-party components under which you intend to install the Metasys Server software as follows: `<alternate path>\Program Files x86\Johnson Controls\Third Party Packages`

   For example: `E:\Program Files x86\Johnson Controls\Third Party Packages`
9. Install the Metasys Server application using the Custom method. In the Install Path field, specify the alternate disk drive in the installation path (for example, E:\Program Files x86). For a unified ADS or ADX, the setup locates, then uses the new databases that you have created. For a split ADX, you select on the installation screens where you placed the databases.

Moving Metasys Historical Databases to a Custom Location

By default, the Metasys Server software and databases are installed to the C: drive. You can move the Metasys historical databases to a different location after you install the Metasys software. Follow the steps in this section.

1. Stop the Metasys III Device Manager service. Open Windows Task Manager. Click the **Services** tab. Right-click the **MIIIDM** service and click **Stop Service**.
2. On the computer that hosts the databases, open SQL Server Management Studio and connect to the database engine computer.
3. In the Object Explorer, expand the **Databases** folder.
4. For each Metasys historical database, right-click on the database and click **Properties**. The Database Properties window appears.
5. In the Select a page pane, click **Files**. Record the paths listed in the Path column of the Database files table. Click **OK** to close the Database Properties window.
6. In the Object Explorer, right-click on the database. Select **Tasks** > **Detach**. The Detach Database window appears.
7. Select the **Drop Connections** checkbox. Click **OK**.

   ⓘ **Note:** A message may appear stating that the database is in use. If this message appears, ensure all Metasys applications are closed and the Metasys III Device Manager service is stopped.
8. Move the .mdf and .ldf database files to the new drive location.
9. After moving the Metasys historical databases, reattach the databases. In the Object Explorer, right-click the **Databases** folder and click **Attach**. the Attach Database window appears.
10. In the Attach Database window, click **Add**. The Locate Database Files dialog box appears.
11. Browse to the new location of the databases. Select the databases and click **OK**.
12. In the Attach Database window, click **OK**. The databases are now attached.
13. If the Metasys historical databases do not appear under the Database folder in the Object Explorer, right click the SQL folder (database engine computer node) and select **Refresh**.

For Johnson Controls technicians: Refer to *FSC Solutions Database Article 30393* for instructions on using a SQL script to complete this procedure.

Configuring Additional Network Cards

About this task:

You can install ADS/ADX and SCT software on a computer that has multiple network cards. If your computer has only one network card, skip this section. If your computer has two or more network cards, follow the steps in this section to specify the network card used for the ADS/ADX and SCT software. Also, for a split ADX, follow these steps to configure the network cards of both computers: the database server and the web/application server.

1. In the **Control Panel**, click **System and Security** > **System** > **Device Manager**. If the **User Account Control** window appears, click **Continue** or **Yes**. The **Device Manager** window appears.
2. Expand the **Network Adapters** item. Both software miniports and hardware network adapters are listed. Consult your computer documentation to determine which items represent physical network cards. You need to know how many physical cards are present in the computer for the next step.
3. If only one physical network card is listed, skip this section. If more than one physical network card is listed, go to the next step.
4. Close **Device Manager**. Return to the **Control Panel** and click **Network and Internet** > **Network and Sharing Center** > **Change Adapter Settings**. The **Network Connections** window appears.

   ⓘ **Note:** If the menu bar is not displayed on the **Network Connections** window, press the Alt key.

5. Click **Advanced** > **Advanced Settings**. The **Advanced Settings** window appears.

   ⓘ **Note:** If the menu bar does not appear, click **Organize**, select **Layout** and then check **Menu bar**.

6. In the **Connections** list, click the network connection that the Metasys system uses. Use the arrow buttons to move the connection to the top position. With the **Adapters and Bindings** tab selected, clear the Internet Protocol Version 6 options if checked.
7. To save the changes, click **OK**.
8. On the **Network Connections** window, right-click the network connection that the Metasys system uses, and select **Properties**. The **Local Area Connection Properties** window appears.
9. Click **Internet Protocol Version 4 (TCP/IPv4)**. Click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears.
10. Click **Advanced**. The **Advanced TCP/IP Settings** window appears.
11. Clear the **Automatic metric** check box (if selected) and, in the **Interface metric** field specify 1. Providing a low Interface metric number to the computer ensures Metasys network traffic has the highest communication priority.
12. To save the changes, click **OK**.
13. Repeat steps 8 through 12 for the second (and each subsequent) active network card on the computer. However, for the second (and each subsequent) active card, increment the Interface metric value **by 1** for each card. Following these steps ensures communication priority between the ADS/ADX and SCT and network engines.
14. Close all windows.

Adding the Metasys Advanced Reporting System to an Existing ADS/ADX

ⓘ **Note:** When you install or upgrade an ADS or ADX computer, you can add support for the Metasys Advanced Reporting System during the normal installation sequence if you have an ADX (or an ADX that was upgraded from an ADS) and SQL Server software that is supported by Metasys software with SQL Server Reporting Services. After you install an ADX without the Metasys Advanced Reporting System, you **cannot** go back and add support for the Metasys Advanced Reporting System without reinstalling the ADX software. Also, after you install the Metasys Advanced Reporting System, it cannot be uninstalled separately using the Add/Remove Programs procedure in Windows.

When in doubt, upgrade your entire system and add SQL Server software that is supported by Metasys software with SQL Server Reporting Services (SSRS) and an ADX that supports the Metasys Advanced Reporting System. For instructions, refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*.

To add the Metasys Advanced Reporting System to an ADS or ADX:

- For an ADS, upgrade to an ADX and select the Metasys Advanced Reporting System option during installation. For instructions, refer to the *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
- For an ADX:
    - If you are using any version of SQL Server software without SQL Server Reporting Services:
        i. Back up all archive databases and all historical databases: JCIAuditTrails, JCIEvents, JCIHistorianDB, JCIReportingDB, SpacesAuthorization and JCIItemAnnotation.
        ii. Uninstall the ADX software using Add/Remove Programs or Uninstall a Program. Do not retain the Metasys databases.
        iii. Uninstall SQL Server software, restart the computer, then reinstall SQL Server software including the supported service pack, making sure you add the Reporting Services component.
        iv. Install the ADX software with Metasys Advanced Reporting System support.
        v. Restore all archive databases and historical databases.
    - If you are using SQL Server software with Reporting Services, uninstall the ADX software using Add/Remove Programs or Uninstall a Program (retaining the databases), then reinstall the ADX software with Metasys Advanced Reporting System support. If you have a split ADX, make sure you have the SQL Server software components installed correctly on all computers. The SCT database can use any version of SQL Server software that is supported by Metasys software.

For steps to install the ADX for Metasys Advanced Reporting System support, see Metasys Server Software.

Changing the Database Referenced by the Metasys Advanced Reporting System

To change the database referenced by the Metasys Advanced Reporting System after you install it, refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*.

Appendix: Metasys Advanced Reporting System Troubleshooting

ⓘ **Note:** For general ADS and ADX installation troubleshooting information, see General Troubleshooting.

For additional troubleshooting information related to SQL Server Reporting Services, go to http://msdn.microsoft.com/en-us/library/ms159135.aspxhttp://msdn.microsoft.com/en-us/library/ms159135.aspx.

Table 57: Metasys Advanced Reporting System Troubleshooting

Problem	Solution
The Trend Summary and Alarm Summary reports do not function properly.	This problem occurs when the SCT computer is inaccessible to the reporting system ADX and the cache cannot refresh. This problem may occur when the SCT computer is offline, in a sleep or hibernating state, or the network card is using the power saving option. To prevent this problem, make sure to set the power options for the SCT computer are properly set. Refer to the *ADS Commissioning Guide (LIT-1201645)* for details about setting the power options.

When you are trying to print a report with the Metasys Advanced Reporting system, this error occurs:
`Unable to load client print control.`
Then when trying to install the required ActiveX control, this error occurs:
`An error occurred during this operation`
	The Microsoft Report Viewer Redistributable package, which is a software prerequisite for the Metasys Advanced Reporting system, is not installed. The installation file is located on the ADS/ADX and SCT installation file. For details, refer to the Microsoft Report Viewer Redistributable Package installation section for your particular version of SQL Server software.
	The second error appears after the first error if you are using a Windows 10, Windows 8.1, or Windows 7 client to browse to the ADS or ADX, and you did not use the Run as Administrator option when you started the browser. Start the browser again using the Run as Administrator option to allow the ActiveX control to install. You only need to perform this step once. After the component is installed, launch the browser using the normal startup process.

One of the following messages appears when you are browsing to `http://localhost/reportserver OR http://localhost/reports:`
`Cannot find the server or DNS error`
`The page cannot be found`
ⓘ **Note:** If you are using a SQL Server named instance other than MSSQLSERVER, the web address includes the suffix _instancename, where instancename is the SQL Server instance name. For example: http://localhost/ReportServer?ThisInstance http://localhost/ReportServer_ThisInstance
	ⓘ **Note:** Make sure you are verifying SQL Server Reporting Services on the correct computer. In a split ADX, this computer is the web/application server computer.
	Start the Reporting Services Configuration Manager for your version of SQL Server software. Verify that each component is configured properly. For details, see *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.

Table 57: Metasys Advanced Reporting System Troubleshooting

Problem	Solution
When you access the reporting system as a non-English user, the content appears in the correct language, but the language is incorrect in the main Toolbar, Report Toolbar, and `Report is being generated` message that appears in the Report screen.	This problem occurs when you do not download the appropriate language support files or restart the appropriate services after the download. Refer to *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
You receive a `The report server is not responding` message when you attempt to verify that SQL Server Reporting Services is running by browsing to one of the following URLs: http://localhost/reportserver http://localhost/reports ⓘ **Note:** If you are using a SQL Server named instance other than MSSQLSERVER, the web address includes the suffix **_instancename**, where **instancename** is the SQL Server instance name. For example: http://localhost/ReportServer$ThisInstance or http://localhost/ReportServer_ThisInstance.	ⓘ **Note:** Make sure you are verifying SQL Server Reporting Services on the correct computer. In a split ADX, this computer is the web/application server computer. Start the Reporting Services Configuration Manager for your version of SQL Server software. Verify that each component is configured properly. For details, refer to *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.

When you attempt to verify that SQL Server Reporting Services is running, you see this message (where 20xx is 2019, 2016, or 2014):
`<SQL Server 20xx error text>Service unavailable:`
`http error 503, the service is unavailable`
	This error occurs only in SQL Server Reporting Services. To resolve, follow these steps:
	1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** > ***Computer Management***. The Computer Management window appears.
	2. In the left pane, expand Local Users and Groups. Select **Groups**.
	3. Under Group names, double-click the **SQLServerReportServerUser** group.
	4. Add the SERVICE and NETWORK SERVICE user accounts to this group. When added, they appear as NT AUTHORITY\SERVICE and NT AUTHORITY\NETWORK SERVICE.
	5. Restart Reporting Services using the Reporting Services Configuration Manager.

Table 57: Metasys Advanced Reporting System Troubleshooting

Problem	Solution
When you attempt to verify that SQL Server Reporting Services is running, you are presented with a Windows Security login prompt, at which time you must enter a user name and password to continue.	Enhanced security in the browser is preventing you from loading the page. Run the Internet Explorer web browser as an administrator (right-click the icon, select **Run** or **Run as Administrator**). Then, try to load the Reporting Services page. If the Reporting Services page still does not appear, log in to the operating system with the **Administrator** account and run the Internet Explorer web browser as an administrator. When the Windows Security login prompt appears, enter Administrator as the user name and the Administrator's password. Wait for the Reporting Services page to appear. Lastly, turn off IE Enhanced Security for the server operating system by following these steps: 1. Start Server Manager. 2. On the Server Manager window, click **Local Server**. 3. In the right column, set the parameter IE Enhanced Security Configuration to **Off**.
When you attempt to verify that SQL Server Reporting Services is running, you see this message: `The report server has encountered a configuration error. (rsServerConfigurationError)`	The Reporting Services log file contains the error **No DSN present in configuration file**. A database connection to Reporting Services has not been created. Start the Reporting Services Configuration Manager for your version of SQL Server software. Click the **Reporting Services Configuration Manager** tile on the Start screen. Follow Step 5 through Step 9 in *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.
When you attempt to verify that SQL Server Reporting Services is running, a scripting error occurs. The message text in the SQL Server Reporting Services window is: `This page might not function correctly because either your browser does not support active scripting or active scripting is disabled.`	Enhanced security in the browser is preventing you from loading the page. Add the computer as a trusted site. For example, if the computer is called ADX-01, add http://ADX-01 to the list of trusted sites under security options for the browser. Alternately, turn off IE Enhanced Security for the server operating system by following these steps: 1. Start Server Manager. 2. On the Server Manager window, click **Local Server**. 3. In the right column, set the parameter IE Enhanced Security Configuration to **Off**.

Table 57: Metasys Advanced Reporting System Troubleshooting

Problem	Solution
You configured SQL Server Reporting Services, but you cannot connect to http://localhost/reportserver or http://localhost/reports. ⓘ **Note:** If you are using a SQL Server named instance other than MSSQLSERVER, the web address includes the suffix **_instancename**, where **instancename** is the SQL Server instance name. For example: http://localhost/ReportServer$ThisInstance or http://localhost/ReportServer_ThisInstance.	Make sure you are verifying SQL Server Reporting Services on the correct computer. In a split ADX, this computer is the web/application server computer. Also, on a split ADX, the Reporting Services Database Setup/ Database Connection has not been configured properly. To resolve this problem, go back to the correct set of wizard overview steps. See *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*
	Errors still exist in the Reporting Services Configuration Manager. To resolve this problem, go back to the correct set of wizard overview steps. See *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*
When you have the Reporting Configuration Manager open for SQL Server software, and make a change under Service Manager, a Backup Encryption Key dialog box appears.	The backup encryption key is not used by Metasys software. However, to satisfy Reporting Services configuration, click the **Browse** button (...), specify a file name for the encryption key, and click **OK**. Specify a password for the file and click **OK**.

The following errors appear in the Event Viewer log:
`Report Server Windows Service <SQL Server instance> cannot connect to the report server database.`
`There was an error starting the Security Authentication/Authorization subsystem. The following database is not functioning properly due to a database error: MetasysIII.`
	The Reporting Service is attempting to connect to the Metasys databases before the databases have completed their startup sequence. Wait 5 to 10 minutes, then verify that Reporting Services has recovered by starting the Internet Explorer web browser and browsing to http://localhost/reportserver.

You are installing SQL Server software with Reporting Services, but the **Install the native mode default configuration** option is unavailable.	This problem may occur when SQL Server software is already installed on the ADX and you install the software again to add Reporting Services. To resolve this problem, follow these steps: 1. Complete the installation. 2. Configure Reporting Services manually. See *SQL Server Software Installation and Upgrade Guide (LIT-12012240)*.

Table 57: Metasys Advanced Reporting System Troubleshooting

Problem	Solution
When you log in to the Metasys Advanced Reporting System for the first time, you see an error message in red text above the Report Selection area.	This situation may occur if you did not add a Site object to the SCT archive before you installed the ADX. To resolve this problem: 1. Log out of the Metasys Advanced Reporting System UI. 2. Open the SCT archive used by the Metasys Advanced Reporting System. 3. Add a Site object to the archive. 4. Log out of the SCT UI. 5. Log in to the Metasys Advanced Reporting System UI.
	This situation may occur if you did not upgrade your SCT archive before you upgraded the ADX. To resolve this problem: 1. Uninstall the ADX software using Add/Remove Programs. 2. Upgrade the archive. 3. Reinstall the ADX.
	For more information, open the Windows Event Viewer and check for errors in the ADSADX Log.

Table 57: Metasys Advanced Reporting System Troubleshooting

Problem	Solution
When attempting to run a report, Metasys Advanced Reporting System does not generate reports. An exception error is logged in the error log.	To prevent this problem, ensure you install the Microsoft and Metasys software components in the correct order. If you install the Microsoft web components and add an SSL certificate before installing the SQL Server Reporting Services (SSRS) component, the SSRS component requires a manual edit to its configuration file in order to function. The SSRS configuration wizard cannot make the correction to the configuration file. To manually edit the configuration file: 1. Go to `C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\Reporting Services\ReportServer` and locate the error log file. ⓘ **Note:** The MSRS10_50.MSSQLSERVER directory name listed in Step 1 is dependent on the SQL Server version and install options. 2. In the error log file, change the Secure Connection Level to the following: 3. `<Add Key="SecureConnectionLevel" Value="0"/>` 4. Save the log file.

Software terms

Use of the software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at www.johnsoncontrols.com/techterms. Your use of this product constitutes an agreement to such terms.

Product warranty

This product is covered by a limited warranty, details of which can be found at www.johnsoncontrols.com/buildingswarranty.

Patents

Patents: https://jcipat.com

Contact information

Contact your local branch office: www.johnsoncontrols.com/locations

Contact Johnson Controls: www.johnsoncontrols.com/contact-us