Contents

Document Introduction...................................................................................................................7
Summary of Changes........................................................................................................................7
Commissioning the ADS Overview.................................................................................................7
Application and Data Server (ADS) and Extended Application and Data Server (ADX).............7
ADS Device Object.............................................................................................................................8
Site Director..........................................................................................................................................10
Repositories..........................................................................................................................................10
  Trend Repository Database..............................................................................................................11
  Audit Repository Database..............................................................................................................12
  Event Repository Database..............................................................................................................12
  Annotation Repository Database......................................................................................................13
  Metasys Reporting Repository Database........................................................................................13
  Spaces Authorization Repository Database......................................................................................13
Message Queue Size Considerations..............................................................................................14
System Security for the ADS/ADX......................................................................................................14
Time Zone, Date, and Time Management........................................................................................15
Email, Pager, SNMP Trap, and Printer Agents.................................................................................15
  Email DDA.................................................................................................................................. 15
  Pager DDA.................................................................................................................................. 15
  SNMP Trap DDA......................................................................................................................... 16
  Printer DDA................................................................................................................................ 16
Syslog DDA....................................................................................................................................... 16
Antivirus Software............................................................................................................................... 19
Printing Information Displayed on the User Interface...................................................................19
Receiving Data from Remote NAEs/NCEs or NIEs............................................................................19
Additional Configuration Notes........................................................................................................19
  An ADS and ADX on the Same Site............................................................................................. 19
  Uninterruptible Power Supply........................................................................................................ 20
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Overview</td>
<td>20</td>
</tr>
<tr>
<td>RADIUS User Accounts</td>
<td>21</td>
</tr>
<tr>
<td>Detailed Procedures</td>
<td>21</td>
</tr>
<tr>
<td>Configuring an ADS/ADX as Site Director</td>
<td>21</td>
</tr>
<tr>
<td>Configuring an ADS/ADX as Site Director with One ADS/ADX</td>
<td>21</td>
</tr>
<tr>
<td>Configuring One ADS/ADX as Site Director with Multiple ADS/ADX Devices</td>
<td>21</td>
</tr>
<tr>
<td>Configuring an ADS/ADX as Site Director if You Delete the Current Site Director</td>
<td>22</td>
</tr>
<tr>
<td>Configuring ADS/ADX Repositories</td>
<td>22</td>
</tr>
<tr>
<td>Sizing the Message Queue</td>
<td>23</td>
</tr>
<tr>
<td>Setting the Time Zone, Date, and Time on an ADS/ADX</td>
<td>24</td>
</tr>
<tr>
<td>Setting Power Options for the ADS/ADX</td>
<td>24</td>
</tr>
<tr>
<td>Setting Power Options for the ADS/ADX Network Card</td>
<td>24</td>
</tr>
<tr>
<td>Setting Power Failure Options for the ADS/ADX</td>
<td>25</td>
</tr>
<tr>
<td>Setting up a Local or Network Printer on an ADS/ADX</td>
<td>25</td>
</tr>
<tr>
<td>Setting up a Local or Network Printer for Scheduled Reports Output</td>
<td>26</td>
</tr>
<tr>
<td>Configuring an ADS/ADX to Accept Dial-Up Connections</td>
<td>27</td>
</tr>
<tr>
<td>Configuring Dial-Up Connections</td>
<td>27</td>
</tr>
<tr>
<td>Removing User Accounts from a Demoted Site Director</td>
<td>28</td>
</tr>
<tr>
<td>Changing the Site Director</td>
<td>28</td>
</tr>
<tr>
<td>Moving the Security Database and Clearing It from the Demoted Site Director</td>
<td>28</td>
</tr>
<tr>
<td>Configuring Metasys System Settings</td>
<td>29</td>
</tr>
<tr>
<td>Changing Metasys Login Screen Background</td>
<td>29</td>
</tr>
<tr>
<td>Changing the Action Queue Timeout</td>
<td>30</td>
</tr>
<tr>
<td>Creating Audit Entries for Discard Events</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Metasys Advanced Reporting System Settings</td>
<td>30</td>
</tr>
<tr>
<td>Refreshing the Metasys Advanced Reporting System Data Manually</td>
<td>30</td>
</tr>
<tr>
<td>Changing Metasys Advanced Reporting System Settings for IIS</td>
<td>31</td>
</tr>
<tr>
<td>Changing the Archive Database Used by the Metasys Advanced Reporting System (Windows Server Platform Only)</td>
<td>32</td>
</tr>
</tbody>
</table>
Verifying the SQL Server Software.................................................................................................... 85
Reinstalling the *Metasys* Software.................................................................................................. 85
Downloading the *Metasys* Archive Database................................................................................. 86
Applying the ADS/ADX/ODS Settings................................................................................................. 87
  ADS Settings................................................................................................................................. 87
Applying the Launcher Settings........................................................................................................ 88
Uploading the *Metasys* Archive Database..................................................................................... 88
Verifying the *Metasys* Advanced Reporting System..................................................................... 89
Appendix: Configuring and Maintaining Preferences...................................................................... 89
  Configuring and Maintaining Preferences Introduction................................................................. 89
Preferences Concepts....................................................................................................................... 90
  System and User Preferences....................................................................................................... 90
  Managing Preferences....................................................................................................................92
Detailed Procedures.......................................................................................................................... 93
  Configuring Preferences............................................................................................................... 93
  Restoring Default System Preferences........................................................................................ 93
  Copying Preferences between Devices....................................................................................... 93
  Restoring Default User Preferences........................................................................................... 94
  Removing User Preference Files................................................................................................. 94
  Copying User Preferences to Another User............................................................................... 94
  Preserving Preferences in an Upgrade......................................................................................... 94
Appendix: Microsoft Windows Operating System and SQL Server Software License Requirements................................................................................................................................. 95
  Windows Operating System License Requirements...................................................................... 95
    Operating System CALs............................................................................................................. 95
    Purchasing and Designating CALs............................................................................................. 96
    Licensing Modes and CAL Examples.......................................................................................... 97
  SQL 2016, SQL Server 2014, and SQL Server 2012 Licensing Requirements................................. 98
  ADS/ADS-Lite or Requirements.................................................................................................... 99
Document Introduction

The ADS/ADX software contains features and configurations that are not set up by the installation or license selection. This document describes the workflow for how to commission the Application Data Server (ADS) or the Extended Application and Data Server (ADX) as part of the Metasys® system, and set up and modify the configuration of the ADS/ADX to better suit the needs of your facility.

For ADS/ADX hardware and software requirements, refer to the Metasys® System Configuration Guide (LIT-12011832).

Note: In this document, the term ADS includes ADS-Lite except where noted. The term NAE includes the NAE45-Lite except where noted. These products are available only to specific markets. Contact your Johnson Controls® representative for details.

Summary of Changes

The following information is new or revised:

- Added clarification for the multiple time zone feature in Multiple Time Zones.
- Added troubleshooting information in ADS/ADX/ODS Stops Responding After Windows Updates.
- Removed SQL Server 2008 and SQL Server 2008 from the document. These versions of SQL Server are no longer supported by Metasys software.
- Updated the Troubleshooting section to include topics on RabbitMQ.
- Added Sync Engine Command Scenarios as an additional Troubleshooting topic for the Online Archive.
- Added the Metasys Services Utilities Introduction section.

Commissioning the ADS Overview

The importance of commissioning the ADS/ADX relates to the Microsoft® Licensing requirements. Refer to http://www.microsoft.com and see Appendix: Microsoft® Windows® Operating System and SQL Server® Software License Requirements for details on licensing. You must also license the ADS/ADX software if you have not already done so. For licensing details, refer to the Software Activation Manager Help (LIT-12012389)

Application and Data Server (ADS) and Extended Application and Data Server (ADX)

The ADS is a scalable platform that serves multiple users and provides database software options for archiving historical data using the Microsoft SQL Server® Express software database.

The extended version of the ADS, the ADX, serves a larger number of users and provides higher capacity historical data storage using the SQL Server software database. The ADX may also be configured in a split configuration, where the web/application components of the ADX reside on a dedicated web/application server and the historical databases of the ADX reside on a dedicated database server. See the following table for ADX split configuration guidelines.
Table 1: ADX Split Configuration Guidelines

<table>
<thead>
<tr>
<th>Product</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADX Web/Application Server</td>
<td>Must be loaded on a full server.</td>
</tr>
<tr>
<td></td>
<td>• Note:</td>
</tr>
<tr>
<td></td>
<td>• ADX software and all required ADX prerequisites reside on a web/application server. Users browse to the web/application server to see system data.</td>
</tr>
<tr>
<td></td>
<td>• You may install Metasys Advanced Reporting System or Energy Essentials on this server.</td>
</tr>
<tr>
<td>ADX Database Server</td>
<td>Must be loaded on a full server.</td>
</tr>
<tr>
<td></td>
<td>• Note: SQL Server software resides on the ADX database server. The database server stores historical Metasys system data and serves as a historical data repository for the web/application server.</td>
</tr>
<tr>
<td>System Configuration Tool (SCT)</td>
<td>Must be loaded on a third server that is separate from the ADX web/application server and ADX database server.</td>
</tr>
</tbody>
</table>

For ADS/ADX hardware and software requirements, refer to the *Metasys® System Configuration Guide* (LIT-12011832).

• **Note:** We recommend that you do not install or run additional software, such as word processors, games, or Computer Aided Drafting (CAD) software, on the ADS/ADX computer. Only install and run the software listed in the *SCT Installation and Upgrade Instructions* (LIT-12012067), *Metasys® Server Installation and Upgrade Instructions* (LIT-12012162) or the *Metasys Server Lite Installation and Upgrade Instructions* (LIT-12012258), including ADS/ADX, SCT, and antivirus software.

**ADS Device Object**

The user interface organizes the ADS device object attributes in the user interface tabs described in Table 2. The **Object Type** and **Model Name** of an ADX are both shown as ADS in the **Focus** window for the ADS device object.
Note: Online refers to the tabs you see when you look at the ADS/ADX user interface. SCT refers to the tabs you see when you look at an archive database in the SCT.

Table 2: User Interface Tabs of the ADS Device Object

<table>
<thead>
<tr>
<th>Tab</th>
<th>Purpose</th>
<th>Online/SCT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus/Configuration</td>
<td>Description of device including information related to site. The tab also includes general information about the ADS Repository, particularly if historical data needs to be forwarded to other ADS Repositories.</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The Focus tab appears online and the Configuration tab appears in the SCT.</td>
</tr>
<tr>
<td>Summary</td>
<td>Name, value, status, and description for Trend Study or User Graphic items in the ADS</td>
<td>Online</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>HTTPS messaging information for diagnostic purposes</td>
<td>Online</td>
</tr>
<tr>
<td>Email</td>
<td>Email configuration and destination information</td>
<td>Both</td>
</tr>
<tr>
<td>Pager</td>
<td>Pager configuration and destination information</td>
<td>Both</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol (SNMP) configuration and destination information</td>
<td>Both</td>
</tr>
</tbody>
</table>
Table 2: User Interface Tabs of the ADS Device Object

<table>
<thead>
<tr>
<th>Tab</th>
<th>Purpose</th>
<th>Online/SCT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog</td>
<td>The Syslog option provides positive indication of each field possible in the Metasys event and auditentries, replacing any blank field with the single character dash (-).</td>
<td>Both</td>
</tr>
<tr>
<td>Printer</td>
<td>Alarm printer configuration and destination information</td>
<td>Both</td>
</tr>
</tbody>
</table>

Site Director

The Site Director provides all users a uniform point of entry to the system and the ability to view all network components, including the information defined in the site object. The Site Director supports functions such as user login, user administration, and time synchronization. Starting at Release 6.5, a remote services connection allows you to connect your Metasys site to cloud-based applications. For more information on how to connect to cloud-based applications, refer to Remote Services Connection in the Metasys® SMP Help (LIT-1201793).

On a Metasys site, only one ADS/ADX server can be configured as the Site Director. All User Views created for a site need to reside on the ADS/ADX configured as the Site Director. Typically, the user graphics created for a site also reside on the Site Director ADS/ADX.

Repositories

Important: The ADS Repository attribute in the engine or server determines where the device sends historical information. The Default ADS Repository attribute in the Site object defines where historical data is stored. By default, these repository attributes are blank. Be sure to enter the address or name of your repository device (typically the Site Director) in these attributes to ensure that you do not lose historical data. For the Site Director itself, leave the ADS Repository attribute blank if the Site Director also serves as the repository. The Default ADS Repository attribute defines the location of the ADS repository for all devices on the site that do not have the ADS Repository attribute defined on their own. The ADS Repository attribute, once defined on an NAE, overwrites the Default ADS Repository attribute of the site for that NAE.

A repository provides long-term storage for historical data. Typically, the ADS/ADX configured as the Site Director also provides the individual repositories for trend data, event messages, audit messages, annotations, reporting, and spaces authorization data. Individual repositories may reside in the SQL Server database. For a split ADX, the repositories are on the database server where the SQL Server software is installed. You can install a split ADX where the database server computer stores all historical data.

Note: The ADS-Lite cannot be a Site Director for other ADS or ADX servers.

The following table lists the ADS/ADX repositories, the corresponding online Metasys® SMP Help (LIT-1201793) or Metasys UI Help (LIT-12011953) topic, and the corresponding file name. The next sections describe the repositories in more detail and suggest ways to optimize the repositories.

Table 3: ADS/ADX Repositories

<table>
<thead>
<tr>
<th>Repository</th>
<th>Refer To</th>
<th>Database File Name on the ADS/ADX Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trends</td>
<td>Trend Extensions in the Metasys® SMP Help (LIT-1201793)</td>
<td>JCIHistorianDB</td>
</tr>
</tbody>
</table>
Table 3: ADS/ADX Repositories

<table>
<thead>
<tr>
<th>Repository</th>
<th>Refer To</th>
<th>Database File Name on the ADS/ADX Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audits</td>
<td>Audit Trail in the <em>Metasys® SMP Help (LIT-1201793)</em></td>
<td>JCIAuditTrails</td>
</tr>
<tr>
<td>Events</td>
<td>Alarm and Event Management in the <em>Metasys® SMP Help (LIT-1201793)</em></td>
<td>JCEvents</td>
</tr>
<tr>
<td>Annotation</td>
<td>Object Message Annotations in the <em>Metasys® SMP Help (LIT-1201793)</em></td>
<td>JCIItemAnnotation</td>
</tr>
<tr>
<td>Annotation Note:</td>
<td><em>Metasys UI does not use this database.</em></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>Advanced Reporting in the <em>Metasys® SMP Help (LIT-1201793)</em></td>
<td>MetasysReporting</td>
</tr>
<tr>
<td><em>Metasys UI Reporting</em></td>
<td>Reporting: Trend Widget and Custom Trend Viewer in the <em>Metasys® UI Help (LIT-12011953)</em></td>
<td>JCIReportingDB</td>
</tr>
<tr>
<td>Spaces Authorization</td>
<td>User Authorization and Dashboard Manager in the <em>Metasys® UI Help (LIT-12011953)</em></td>
<td>SpacesAuthorization</td>
</tr>
</tbody>
</table>

**Trend Repository Database**

**Trend Repository Overview**

The Trend repository database resides on the ADS/ADX within the SQL Server software database. The installation program places the Trend repository on the same computer where the ADX software resides. The default directory location is `C:\ProgramData\Johnson Controls\MetasysIII\SQLData` (pre-Release 8.0) or `C:\Program Files\Microsoft SQL Server\MSSQL\version\MSSQLSERVER\MSSQL\DATA` (Release 8.0 or later). For a split ADX, the directory location is on the database server on the same drive where the SQL Server software is installed. If you want to change where the databases are loaded (for example, `E:\MyDatabases`), you need to do so before you install the ADS/ADX software. For details, refer to the *Metasys® Server Installation and Upgrade Instructions Wizard (LIT-12012162)* or the *Metasys Server Lite Installation and Upgrade Instructions (LIT-12012258)*.

The ADS/ADX performance degrades as the number of Trend samples coming in to the ADS/ADX Trend repository increases. In addition, the frequency of the trend samples to be stored in the Trend repository increases, depending on the hardware resources used for the ADS/ADX computer.

**Trend Repository Optimization**

Optimize the required storage size of the ADS/ADX Trend repository using the following methods:

- configure larger sample intervals for individual trends
- determine which trends to store long-term and transfer only these samples
- configure the trends of non-critical objects to sample on large Change-of-Value (COV) increments

In addition, optimize the network communication performance for transferring trend samples from NAE/NCE or NIE devices to the ADS/ADX repository using the following methods:

- configure the Transfer Setpoint on individual trends so they transfer their samples at intervals different from other trends
- use the ADS Delivery Time of the Network Automation Engine (NAE)/Network Control Engine
(NCE) or Network Integration Engine device to transfer the samples at the time when user access to the system is minimal.

Refer to the Trend Extensions topic in the Metasys® SMP Help (LIT-1201793) for more information.

Audit Repository Database

Audit Repository Database Overview

The Audit Repository resides on the ADS/ADX within the SQL Server software database. The installation program places the Audit repository on the same computer where the ADX software resides. The default directory location is C:\ProgramData\Johnson Controls\MetasysIII\SQLData (pre-Release 8.0) or C:\Program Files\Microsoft SQL Server\MSSQL\version>.MSSQLSERVER\MSSQL\DATA (Release 8.0 or later). For a split ADX, the directory location is on the database server computer on the same drive where the SQL Server software is installed. If you want to change where the databases are loaded (for example, E:\MyDatabases), you need to do so before you install the ADS/ADX software. For details, refer to the Metasys® Server Installation and Upgrade Instructions Wizard (LIT-12012162) or the Metasys Server Lite Installation and Upgrade Instructions (LIT-12012258).

The ADS/ADX performance degrades as the number of audit samples coming in to the ADS/ADX Audit repository increases. In addition, the frequency of the audit samples to be stored in the Audit repository increases, depending on the hardware resources used for the ADS/ADX computer.

Audit Repository Optimization

Optimize the required storage size of the ADS/ADX Audit repository by specifying the Audit level (1 through 4) for the audit messages that need to be reported and archived.

In addition, optimize the network communication performance for transferring audit messages from NAE/NCE or NIE devices to the ADS/ADX Event repository by optimizing the Audit repository size in the device object of each NAE/NCE or NIE.

Audit Level 1 provides the minimum information. Audit Level 4 provides the most information. Audit Level 2 is the default setting. Refer to the Audit Trail topic in the Metasys® SMP Help (LIT-1201793) for more information.

Event Repository Database

Event Repository Overview

The Event repository resides on the ADS/ADX within the SQL Server software database. You may view and acknowledge ADS/ADX alarms and events in the event repository. The newest and highest priority alarm or event that requires acknowledgment appears in the Alarms window. Use the Event Viewer to see all the events in a device repository. When the device repository receives an acknowledgment either from the user interface or through a web service, the original source device of the alarm is notified.

The installation program places the Event repository on the same computer where the ADX software resides. The default directory location is C:\ProgramData\Johnson Controls\MetasysIII\SQLData (pre-Release 8.0) or C:\Program Files\Microsoft SQL Server\MSSQL\version>.MSSQLSERVER\MSSQL\DATA (Release 8.0 or later). For a split ADX, the directory location is on the database server computer on the same drive where the SQL Server software is installed. If you want to change where the databases are loaded (for example, E:\MyDatabases), you need to do so before you install the ADS/ADX software. For details, refer to the Metasys® Server Installation and Upgrade Instructions Wizard (LIT-12012162) or the Metasys Server Lite Installation and Upgrade Instructions (LIT-12012258).

The ADS/ADX performance degrades as the number of event samples coming into the ADS/ADX Event repository increases. In addition, the frequency of the event samples to be stored in the Event repository increases, depending on the hardware resources used for the ADS/ADX computer.
Event Repository Optimization

Optimize the required storage size of the ADS/ADX Event repository by only defining intrinsic alarming, Event Enrollment objects, or alarm extensions for point objects for which event messages need to be processed and archived.

In addition, optimize the network communication performance for transferring event messages from NAE/NCE or NIE devices to the ADS/ADX Event repository by optimizing the Alarm repository size in the device object of each NAE/NCE or NIE.

Refer to the Alarm and Event Management section in the Metasys® SMP Help (LIT-1201793) for more information.

Annotation Repository Database

The Annotation repository resides on the ADS/ADX within the SQL Server software database. The Annotation repository contains all optional annotations entered manually for items in the All Items tree.

The installation program places the Annotation repository on the same computer where the ADX software resides. The default directory location is C:\ProgramData\Johnson Controls\MetasysIII \SQLData (pre-Release 8.0) or C:\Program Files\Microsoft SQL Server\MSSQL<version>\MSSQLSERVER \MSSQL\DATA (Release 8.0 or later). For a split ADX, the directory location is on the database server computer on the same drive where the SQL Server software is installed. If you want to change where the databases are loaded (for example, E:\MyDatabases), you need to do so before you install the ADS/ADX software. For details, refer to the Custom Locations for Metasys Server Application and Databases section in the Metasys® Server Installation and Upgrade Instructions Wizard (LIT-12012162).

The ADS/ADX performance degrades as the number of annotations coming in to the ADS/ADX Annotation repository increases and the frequency of the annotation samples to be stored in the Annotation repository increases, depending on the hardware resources used for the ADS/ADX computer. The Annotation repository requires no special optimization because the repository only grows in size as the number of annotations increases.

Metasys Reporting Repository Database

The Metasys Reporting repository database resides on an ADS/ADX within the SQL Server software database. The Metasys Reporting repository contains Metasys Advanced Reporting System information and Metasys Energy Essentials configuration information.

The installation program places the Metasys Reporting repository on the same computer where the ADX software resides. The default directory location is C:\ProgramData\Johnson Controls\MetasysIII \SQLData (pre-Release 8.0) or C:\Program Files\Microsoft SQL Server\MSSQL<version>\MSSQLSERVER \MSSQL\DATA (Release 8.0 or later). For a split ADX, the directory location is on the database server computer on the same drive where the SQL Server software is installed. If you want to change where the databases are loaded (for example, E:\MyDatabases), you need to do so before you install the ADS/ADX software. For details, refer to the Custom Locations for Metasys Server Application and Databases section in the Metasys® Server Installation and Upgrade Instructions Wizard (LIT-12012162).

Spaces Authorization Repository Database

Spaces Authorization Repository Database Overview

The Spaces Authorization Repository resides within the SQL Server software database. The folder location of the database files that store authorization data is selected during the Metasys server installation. The default directory location is C:\Program Files\Microsoft SQL Server \MSSQL<version>\MSSQLSERVER\MSSQL\DATA (Release 8.0 or later).

Note: The installation program places the Spaces Authorization repository on the same computer where the ADX software resides. For a split ADX, the directory location is on the database server on the same drive where the SQL Server software is installed. If you want to change where the databases are loaded (for example, E:\MyDatabases), you need to do
so **before** you install the ADS/ADX software. For details, refer to the Custom Locations for Metasys Server Application and Databases section in the *Metasy® Server Installation and Upgrade Instructions Wizard (LIT-12012162)*.

**Message Queue Size Considerations**

Microsoft Message Queuing (MSMQ) is an optional feature in Windows® operating systems that supports reliable, persistent storage of messages that require processing when the recipient device is temporarily offline or busy. Message queuing is implemented in the *Metasy* system on the ADS/ADX to support alarming, trending, and Site Management Portal user interface navigation tree features. The Site Director queue receives events, trend data, and navigation tree changes from other system devices. When the Site Director is busy, the messages remain in the queue until the Site Director is available to process them. Message queuing allows the system to avoid bottlenecks by separating the actions of receiving and processing data. For more information on MSMQ functions in the *Metasy* system, refer to the *Network and IT Guidance for the BAS Professional Technical Bulletin (LIT-12011279)*.

The current default MSMQ queue size limitation is 1 GB. The backlog queue used to store trend messages is limited to 900 MB. The default queue size may be inadequate if your site is trending large amounts of data, trend repositories go offline, or if an ADS/ADX is unavailable to the network for long periods of time. If MSMQ does not function correctly, your system may lose trend information. We recommend that you manually resize the message queue for your site if one of the following criteria applies:

- You are trending near 100,000 trend samples per hour.
- Your backlog queue is 50% full on a regular basis.
- You are forwarding trend information from one ADS/ADX to another destination.

**Note:** To find out if you are forwarding trend information, browse to the ADS/ADX user interface. If the ADS Repositories attributes value is Listof\[x\], where x is a number greater than zero, you are forwarding trend information. The destination could be an ADS/ADX user interface.

To set the size of the message queue, see *Sizing the Message Queue*.

**System Security for the ADS/ADX**

The Security Administration System protects access to the ADS/ADX and requires users to enter a user ID and complex password when logging in to the ADS/ADX. For details, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)* or the Change Password topic in *Metasy® SMP Help (LIT-1201793)*.

*Metasy* system complex passwords must meet the complexity requirements.

- The password must include a minimum of 8 characters and a maximum of 50 characters.
- The password cannot include spaces or include a word or phrase that is in the Blocked Words list.
- The password and the username cannot share the same three consecutive characters.
- The password must meet the four following conditions:
  - Include at least one number (0–9)
  - Include at least one special character (~, ., @, #, !, ?, $, %)
    **Note:** Only the special characters listed above can be used; all other special characters are invalid.
  - Include at least one uppercase character
A user with the Administrator Role can edit the security database by adding users, modifying user IDs and passwords, and assigning object category-based privileges and system access privileges.

When the ADS/ADX is the Site Director, its Security Administration System function controls access to the entire site. The assigned object category-based privileges and system access privileges affect the permissions granted for the user logged in to the Site Director.

The ADS/ADX also allows you to log in using the Microsoft Active Directory® service. At Release 8.1 and later, the User Principal Name (UPN) authentication support for the Metasys system is now in compliance with Microsoft Office 365 authentication. For details, refer to the Security Administrator System Technical Bulletin (LIT-1201528).

When the ADS/ADX is not the Site Director (used only as a repository for data storage), its local Security Administration System function is used for user authentication for direct access to this ADS/ADX. The assigned system access privileges affect the permissions granted for the user who is directly logged in to this ADS/ADX. The Site Director, where users normally log in to the system, provides the effective Security Administration System function for site-wide access. On sites with multiple ADS/ADX devices, the Site Director security database must be copied to all of the other ADS/ADX devices to support the latest alarm and event features. For information on backing up and copying security databases, refer to the Metasys® SCT Help (LIT-12011964). 

Note: The ADS-Lite cannot be the Site Director for other ADS or ADX servers.

The Security database can only be viewed and modified in the online system at the Site Director by a user with the Administrator Role. If you want to maintain the same Security database for all ADS/ADX devices, back up the archive database (which includes the Security database) of the Site Director with the SCT and then copy this Security database to all ADS/ADX devices on the site.

For more information on System Security, including setting up roles and users, refer to the Security Administrator System Technical Bulletin (LIT-1201528).

We recommend that you implement trusted security certificates for improved protection of user passwords when using the Metasys Advanced Reporting System. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for details on how to implement SSL security.

Time Zone, Date, and Time Management

See Setting the Time Zone, Date, and Time on an ADS/ADX for information on time zone, date, and time management on your network.

Email, Pager, SNMP Trap, and Printer Agents

The ADS/ADX uses an agent called the Destination Delivery Agent (DDA) to route event messages to other media and devices, such as email or a pager. The ADS/ADX supports the DDAs in this section.

Note: For details on how to configure the DDA, refer to the Metasys® SMP Help (LIT-1201793).

Email DDA

The Email DDA supports the standard Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Secure Socket Layer (SSL), and Internet Message Access Protocol (IMAP) for sending event messages to an email account. For details on how to configure the Email DDA, refer to the Metasys® SMP Help (LIT-1201793).

The Email DDA maintains a log file of recent communication. For more information, see Using Communication Log Files.

Pager DDA

The Pager DDA supports the standard Telocator Alphanumeric Protocol (TAP) for sending event messages to a pager. For details on how to configure the Pager DDA, refer to the Metasys® SMP Help (LIT-1201793).
The ADS/ADX does not support modems on the serial port.
The Pager DDA maintains a log file of recent communication. For more information, see Using Communication Log Files in Troubleshooting.

SNMP Trap DDA

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. SNMP monitoring is typically used for large Building Automation System (BAS) networks with many network devices. Alarm and event notifications are sent to and stored on an SNMP management server that monitors all devices on the network.

The ADS/ADX uses the SNMP protocol to deliver network device status and conditions to a designated SNMP management server. SNMP monitoring must be set up at the network level, and an SNMP management server must be assigned on the network. If you are applying a Metasys system to an existing network, consult with the network administrator or IT department that administers the network to determine if SNMP monitoring is available on the network.

Configure custom SNMP messages and specify the SNMP message destinations in the SNMP tab of the SMP UI. Perform this configuration to each ADS/ADX individually. Take note that for the ADS/ADX, SNMP communication is only one way. That is, the SNMP management server can receive network device status and conditions from the ADS/ADX, but it cannot request information from the ADS/ADX or discover the ADS/ADX using the SNMP protocol. This behavior is reflected in the SMP UI as follows: under the SNMP tab of the ADS/ADX, the Destination Port Number attribute is effective, but the SNMP Request Port attribute is ignored.

The ADS/ADX provides enhanced SNMP functionality on Metasys systems, including a Metasys system Management Information Base (MIB) file for configuring third-party SNMP translation applications to request, receive, and translate specified SNMP trap messages generated by the Site Management Portal (SMP) user interface SNMP DDA.

Printer DDA

The Printer DDA is only available on the ADS/ADX for sending event messages to printers. The Printer DDA supports any printer type supported by the Windows operating system on which the ADS/ADX is installed. The Printer DDA also supports IP-based network printers (but not Novell® NetWare printers) and printers that are connected to the ADS/ADX by parallel or USB port. The ADS/ADX supports printing to multiple printers at one time.

Syslog DDA

An ADS/ADX configured as a Site Director has the optional capability of sending its configured audit log entries and alarm notifications to the central repository of an external, industry-standard, Syslog server, conforming to Internet published RFC 3164. After you save the Syslog DDA configuration, all messages that are sent to the local ADS Repository are also sent immediately to the configured Syslog server. You can then open a user interface at the Syslog server and use the provided filters to interrogate or apply forensic analysis on these messages. To assist in reading the log, a vertical bar symbol (|) separates individual fields of each Metasys message and a single character dash (-) replaces any blank field.

By default, the Syslog option is disabled. Changing the Syslog Reporting Enabled attribute to True on the Syslog window enables the Syslog function. The prerequisites to the Syslog DDA are as follows:

- The Syslog server must be installed and running on a computer server or virtual machine that is reachable by the ADS/ADX.
- The ADS/ADX must be running Release 8.0 software or later.
- No more than three Syslog destinations can be specified.
- The firewall port must be open.
The definition of the Syslog DDA requires:

- Label to identify the Syslog server
- IP address of the Syslog server
- Port numbers for the UDP send port and UDP receive port (for example, 514 for both)
- Event and audit filters to apply against all events and audit messages. Only those events and audit messages that match the filters are passed to the Syslog server.

The Syslog DDA attribute called **Syslog Reporting Enabled** appears on the Shared Configuration section of the Syslog tab of an ADS/ADX device object (Figure 2). This attribute has two selections: True or False.

When the Syslog Reporting Enabled attribute is set to True, the feature is active and your Metasys messages (events and audits) are forwarded to your destination Syslog server according to the filtering you specified. When the Syslog Reporting Enabled attribute is set to False, the feature is inactive and no Metasys messages are forwarded to the Syslog server. The configuration example in Figure 2 is set to route to the Syslog server all High Warning alarms that require acknowledgment.

The Syslog DDA implementation is UDP, not TCP. Therefore, any audits/events generated while the Syslog server is offline are not recorded at the Syslog server, even though the Metasys system, unable to determine the current status of the Syslog server, continues to send out messages. A gap in time is present between events when the Syslog server comes back online.

**Figure 2: Syslog Tab in Engine's Device Object**
Figure 3 shows an example of Metasys system messages as they appear on the Kiwi Syslog® Server Console user interface. Use the console to filter the messages. If you do not have a tool, open a web browser and type the following URL:

http://<IP of the server>::<Port>/Events.aspx

For example:

https://SysLogserver1:8088/Events.aspx

When you browse to this site, type a valid username and password when prompted to gain access to the Syslog server. A user interface appears with the captured messages.

If you run into any trouble while implementing the Syslog DDA functionality, consult this following table.

Table 4: Syslog Server Troubleshooting

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The engine is starting up but the SysLog DDA has not yet started.</td>
<td>All generated audits and events are cached and sent to Syslog DDA once it is started. The maximum size of the cache is 1,000 audits and 1,000 events per hour.</td>
</tr>
<tr>
<td>The Syslog server crashes.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached.</td>
</tr>
<tr>
<td>The Syslog server goes offline or is unreachable.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until it comes back online or becomes reachable.</td>
</tr>
<tr>
<td>The IP address, name, or port numbers of the Syslog server as defined in the engine's object are invalid.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until you correct the invalid parameters in the Syslog DDA.</td>
</tr>
<tr>
<td>The Syslog Reporting Enabled parameter is set to True, but no Syslog parameters are defined.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until you specify the parameters that the Syslog DDA requires.</td>
</tr>
</tbody>
</table>
Table 4: Syslog Server Troubleshooting

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The UDP Send Port or UDP Receive Port is blocked by a firewall.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until the ports on the Syslog server are opened.</td>
</tr>
<tr>
<td>A parameter of the Syslog server changes, but the corresponding parameter in the Syslog DDA of the engine is not likewise changed.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is received at the Syslog server until you correct the invalid parameters in the Syslog DDA.</td>
</tr>
</tbody>
</table>

Antivirus Software

Frequent virus scans of the computer running the ADS/ADX are necessary to maintain the integrity of your system. We recommend one of the following antivirus software programs:

- Symantec® Endpoint Protection software Corporate Edition Version 12.0 or later
- McAfee® VirusScan® Enterprise version 8.8 with Patch 9 or higher.

For details, see Appendix: Installing Antivirus Software.

Printing Information Displayed on the User Interface

Any printer supported by the computer's operating system can be used to print the content of any panel displayed on the SMP user interface. The supported printers include IP network printers and printers connected using a USB or parallel port. Printing through Novell NetWare services is not supported.

Receiving Data from Remote NAEs/NCEs or NIEs

Through the use of a dial-up connection, an ADS/ADX may be configured to receive and store trend, alarm, and audit data from individual, remote NAEs/NCEs/NIEs that are not on the same site as the ADS/ADX.

Each remote NAE/NCE/NIE must have its own modem, and each NAE/NCE/NIE must be configured to dial the ADS/ADX. Refer to Configuring an NAE to Dial Out to an ADS/ADX/ODS in the NAE Commissioning Guide (LIT-1201519) for information on setting up an NAE/NIE to dial an ADS.

To use a Multi Tech® MT5634ZBA-USB 56k, V.90 external USB modem in Metasys system networks requires the 8.27L Version or higher of the Multi Tech modem firmware installed on the modem.

The ADS/ADX does not support modems on the serial port.

The ADS/ADX must also be configured to accept incoming dial-up connections. See Configuring an ADS/ADX to Accept Dial-Up Connections. Refer to the Metasys System Extended Architecture Direct Connection and Dial-Up Connection Application Note (LIT-1201639) for details on how to set up a computer to connect directly or by using a dial-up connection to an NAE/NCE/NIE device.

Additional Configuration Notes

When configuring your Metasys system site, consider the notes in this section.

An ADS and ADX on the Same Site

While it is possible to install both an ADS and an ADX on the same site (with the restriction that an ADS-Lite cannot be the Site Director for any other ADSs or ADXs), historical data cannot be shared.
between the two computers. The repository files only exist on one ADS/ADX computer or on the
database server computer in the split ADX. The NAE/NCE/NIE can send historical records to only
one repository computer.

Uninterruptible Power Supply

It is best practice to connect the ADS/ADX to a reliable Uninterruptible Power Supply (UPS) to avoid
data loss in the event of a power outage. Contact your Johnson Controls representative or see the
computer price list on the Johnson Controls employee portal website for UPS recommendations.

RADIUS Overview

You can optionally configure the secured server and network engines to authenticate non-local user
access through a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS is used by
the server and network engines to authenticate the identity of authorized non-local users of the
system.

All RADIUS users must have a Metasys system user defined for which Metasys authorization is
created and maintained. The server and network engines RADIUS implementation adheres to the
following Internet RFC documents:

- RFC 2865 - Remote Authentication Dial In User Service
- RFC 2548 - Microsoft Vendor-specific RADIUS Attributes
- RFC 2759 - Microsoft Point-to-Point Protocol (PPP) Challenge Handshake Authentication Protocol
  (CHAP) Extensions, Version 2

The Metasys system implementation of RADIUS is as follows:

- The Metasys system does not import authorization; all Metasys system users, both local (Metasys)
  and non-local (RADIUS), are authorized through user configuration done online in the SMP, then
  stored in the Metasys Security Database.
- The user ID must match what is expected to be authenticated by the RADIUS server, with or
  without the @domain as defined by the local RADIUS implementation.
- Since the Metasys system performs no local authentication of non-local users, all password
  functions are unavailable or ignored when creating and maintaining non-local Metasys user
  accounts. RADIUS passwords are never stored in the Metasys Security Database.
- Authorization for a RADIUS user may be configured as Administrator, User, Operator,
  Maintenance, or any custom roles created in the Metasys system.
- When a non-local user receives a number of consecutive RADIUS failures to authenticate and
  the account has been set up to lock after receiving that many failed login attempts, the Metasys
  system authorization locks, prohibiting the user from accessing the Metasys system device until a
  Metasys system administrator unlocks the account.
- When a non-local user is authenticated by RADIUS, and the Metasys system schedule prohibits
  access during the login time, the user's login attempt fails.

When a user provides a non-local username to the Metasys system for login, after confirming the
supplied password conforms to Metasys complexity rules, the controller passes the credentials,
including the username and password, to the configured RADIUS server for authentication. After
the RADIUS server confirms authenticated access, authorization is permitted as specified in the
Metasys Security Database.

Messages reporting errors in RADIUS authentication are intentionally obscure to hinder possible
intrusion from unauthorized users. See RADIUS Errors for some situations that may result in error
messages. Descriptive Metasys system login failure messages are presented to the user only when
RADIUS is disabled. When RADIUS is enabled, local and non-local authentication failure messages are identical and obfuscated.

**RADIUS User Accounts**

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and account management for users who connect to and use a network service. RADIUS accounts may be used within MVE environments for electronic signatures and authentication. Users select RADIUS on the SMP UI login screen, similar to Active Directory.

**Detailed Procedures**

**Configuring an ADS/ADX as Site Director**

The ADS/ADX installation process defaults each ADS/ADX to be its own Site Director. When adding multiple ADS/ADX devices to a site for providing additional repositories, only one ADS/ADX can be configured as the Site Director.

⚠️ **Note:**

- The ADS-Lite cannot be the Site Director for any other ADS or ADX servers.
- If an ADS/ADX is already designated as the Site Director, you must first remove the Site Director designation from that ADS/ADX. Use this procedure for the current Site Director and clear Site Director in Step 3. Then repeat as directed for the new Site Director.

1. From the ADS/ADX user interface, open the Site object.
2. Click **Edit**.
3. In the Site Director drop-down list, select the correct Site Director.
4. Click **Save**.

**Configuring an ADS/ADX as Site Director with One ADS/ADX**

By default, a single ADS/ADX on the site is the Site Director.

**Configuring One ADS/ADX as Site Director with Multiple ADS/ADX Devices**

To configure one ADS/ADX as Site Director with multiple ADS/ADX devices, use the System Configuration Tool (SCT) and define all ADS device objects and the Site objects. The first Metasys server (ADS/ADX) inserted into the SCT archive database automatically becomes the Site Director. If you define multiple Metasys servers (ADS/ADX devices), the top Metasys server shown in the All Items navigation tree of the SCT archive database automatically becomes the Site Director.

⚠️ **Note:**

- The ADS-Lite cannot be the Site Director for any other ADS or ADX servers.
- After completing the system configuration, perform a download to all ADS/ADX servers with the SCT to ensure that only the ADS/ADX defined in the Site object is configured as the Site Director and all other ADS/ADX servers are configured as repositories.

If necessary, change the Site Director in the Site object. See **Configuring an ADS/ADX as Site Director**.
Configuring an ADS/ADX as Site Director if You Delete the Current Site Director

If you define multiple Metasys servers (ADS/ADX devices) and you delete the ADS/ADX that is defined as the Site Director, the top Metasys server shown in the All Items navigation tree of the SCT archive database automatically becomes the Site Director.

① **Note:** The ADS-Lite cannot be the Site Director for any other ADS or ADX servers.

If necessary, change the Site Director in the Site object. See Configuring an ADS/ADX as Site Director.

① **Note:** After completing the system configuration, perform a download to all ADS/ADX devices with the SCT to ensure that only the ADS/ADX defined in the Site object is configured as the Site Director and all other ADS/ADX servers are configured as repositories.

Configuring ADS/ADX Repositories

The three typical configurations are as follows:

- The ADS/ADX is the Site Director and the ADS repository.
- The ADS/ADX is the Site Director and a different ADS is the ADS repository.
- The ADX is split so the web/application server computer is the site director and the database server computer is the repository.

① **Note:** Even though the database server computer hosts the Repository, each NAE/NCE/NIE is configured to have its repository entry directed to the ADX web/application server computer. The ADX web/application server accepts the data from the NAE/NCE/NIE and then writes the data to the repository on the database server computer. An NAE/NCE/NIE and the database server computer never communicate directly.

1. Open the ADS object.
2. Set the objects and devices according to Table 5.

① **Note:** Each ADS/ADX that is configured as a repository has the capability to forward the historical data (trend samples and alarm/event messages) received from an NAE/NCE/NIE device to other ADS/ADX repositories as defined in the Repository Storage (list) in its device object. The ADS/ADX does not forward Audit Trails.

Table 5: Configuring ADS Repositories

<table>
<thead>
<tr>
<th>Condition</th>
<th>Device or Object</th>
<th>In This Field</th>
<th>Enter This Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the ADS/ADX Is Both the Site Director and the ADS Repository</td>
<td>On the ADS/ADX (Site Director)</td>
<td>Local Site Director</td>
<td>Its own computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADS Repositories</td>
<td>Not used - leave blank</td>
</tr>
<tr>
<td></td>
<td>On an NAE</td>
<td>Local Site Director</td>
<td>The computer name of the Site Director</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADS Repository</td>
<td>The computer name of the Site Director</td>
</tr>
<tr>
<td>If an ADS/ADX Is the Site Director and a Different ADS Is the ADS Repository</td>
<td>On the ADS/ADX (Site Director)</td>
<td>Local Site Director</td>
<td>Its own computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADS Repositories</td>
<td>The computer name of the ADS Repository</td>
</tr>
</tbody>
</table>
### Table 5: Configuring ADS Repositories

<table>
<thead>
<tr>
<th>Condition</th>
<th>Device or Object</th>
<th>In This Field</th>
<th>Enter This Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the ADS/ADX (ADS Repository)†</td>
<td>Local Site Director</td>
<td>The computer name of the Site Director</td>
<td></td>
</tr>
<tr>
<td>On an NAE or Any Other ADS</td>
<td>Local Site Director</td>
<td>The computer name of the Site Director</td>
<td></td>
</tr>
<tr>
<td>If the ADX Is Split and the Web/Application Server Computer Is the Site Director and the Database Server Computer Is the Repository</td>
<td>On the ADS/ADX (Site Director)</td>
<td>Local Site Director</td>
<td>Its own computer name</td>
</tr>
<tr>
<td></td>
<td>ADS Repositories</td>
<td>Not used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the NAE or Any Other ADS</td>
<td>Local Site Director</td>
<td>The computer name of the Site Director</td>
</tr>
<tr>
<td></td>
<td>ADS Repository(ies)</td>
<td>The computer name of the ADS Repository</td>
<td></td>
</tr>
</tbody>
</table>

† If an ADS/ADX is the repository for all NAE/NIE devices, verify that its computer name is entered as Default ADS Repository in the Site object and also as Default ADS Repository in all NAE/NIE device objects. If this ADS/ADX is the repository only for particular NAE/NIE devices, verify that its computer is entered as ADS Repository only for these NAE/NIE device objects.

2 The ADX web/application server actually accepts the data from the NAE/NIE and then writes the data to the repository on the database server computer.

### Sizing the Message Queue

- **Note:** Message queue sizing is only necessary for systems that meet the criteria outlined in Message Queue Size Considerations.

1. On the ADS/ADX computer, hold down the **Windows** key and press **R**. The Run dialog box appears.
2. Type `compmgmt.msc` in the Open line and press **Enter**. The Computer Management window appears.
3. In the tree on the left, browse to **Services and Applications > Message Queuing > Private Queues**.
4. Right-click `metasys_trendbacklog` and select **Properties**. The metasys_trendbacklog Properties window appears.
5. In the text box next to Limit message storage to (KB), type 10490000.
6. Click **OK**.
7. If you have an ADX computer:
   a. In the tree on the left, right-click **Message Queuing** and select **Properties**. The Message Queuing Properties window appears.
   b. Under Storage limits, clear the check box for Limit message storage to (KB).
c. Click **OK**.

8. Restart the ADS/ADX computer.

9. Repeat this procedure on all other ADSs/ADXs on your site.

### Setting the Time Zone, Date, and Time on an ADS/ADX

See Appendix: Time Zone, Date, and Time Management for information on setting the time zone, date, and time management on your network.

### Setting Power Options for the ADS/ADX

1. In Control Panel, select **Hardware** or **Hardware and Sound**, then **Power Options**. The Power Options dialog box appears.

2. Select the **Create a power plan** option in the left pane. If the User Account Control window appears, click **Allow**.

3. Select the **High Performance** plan. Click **Next**.

4. Select a number of minutes for turning off the display or leave the default of 15 minutes. If you have the **Put the Computer to Sleep** option, select **Never**. Click **Create**.

5. Click the **Change plan settings** option for the custom plan you just created and select the **Change advanced power settings** option. The Power Options dialog box appears.

6. Expand the **Hard disk** option and under the **Turn off hard disk after** setting, either enter **0** in the dialog box or click the down arrow until **Never** is displayed.

7. Expand the **Sleep** option and under the **Hibernate after** setting, select **Never**. Some computers may not provide this setting.

   ○ **Note:** If you are installing on a laptop computer, you may see more than one drop-down selection box for the computer when receiving power and when on battery power. Select **Never** in both boxes.

8. Click **OK** to close the Power Options dialog box. Close all windows.

9. In Control Panel, go to **System and Security > System**, and then select **Advanced system settings**. Click **Continue** or **Yes** if prompted for consent. The System Properties window appears.

10. On the Advanced tab, in the Startup and Recovery section, click **Settings**. The Startup and Recovery box appears.

   ○ **Note:** If you do not see this selection or box, go to Step 12.

11. In the **System failure** section, select the **Automatically restart** option.

12. Click **OK**.

13. Close the System Properties window.

### Setting Power Options for the ADS/ADX Network Card

1. In Control Panel, select **System and Security, System**, then click **Device Manager** in the left pane. If the User Account Control window appears, click **Continue** or **Yes**. The Device Manager
window appears.

2. Expand the **Network Adapters** item.

3. Right-click the network card and then click **Properties**.

4. Select the **Power Management** tab. Clear the option **Allow the computer to turn off this device to save power**.

5. Click **OK**.

6. Close all windows.

### Setting Power Failure Options for the ADS/ADX

Follow these steps to make sure your computer comes back online after a power failure. This procedure requires that you access the computer’s BIOS settings while the computer is starting up. Accessing and changing BIOS settings may vary depending on the computer you are using. Seek input from the IT department if you are unsure how to change the computer’s BIOS settings.

**Note:** You may wish to use an Uninterruptible Power Supply (UPS) to prevent your computer from going offline during a power failure.

1. Restart the computer. While the computer is starting up, press the appropriate key to enter Setup mode (for example, **F10**).

2. Edit the appropriate Power Management settings so the computer restarts after a power failure (for example, set **After Power Failure** to **Switch On**).

3. Save changes and exit Setup mode.

### Setting up a Local or Network Printer on an ADS/ADX

**Note:** This procedure sets the printer as the destination for the Printer DDA.

1. Make sure the printer power is on and is connected to the computer or building network.

2. In Control Panel, click **Hardware and Sound**.

3. Click **Devices and Printers**.

4. Click **Add a Printer** to start the Add Printer Wizard. The **Choose a local or network printer** screen appears. In Windows 7, this screen has the same content but is labeled **What type of printer do you want to install?**

5. Click **Add a local printer** (even if the printer is a network printer). The **Choose a printer port** screen appears.

6. For a network printer, click **Create a new port** and select **Standard TCP/IP Port** from the drop-down list. Go to Step 7.

   For a local printer, select **Use an existing port** and select the appropriate port from the list. Go to Step 8.

7. Click **Next**. The **Type a printer hostname or IP address** screen appears.

8. Enter the host name or IP address of the printer. The **Port name** field autofills while you type the host name or IP address. Keep the **Query the printer** check box selected (the default).
Note: If you are uncertain about the proper printer host name to use, print a test page from the printer and look for the Printer name line in the test printout. Copy the name and syntax exactly. You may otherwise specify the IP address of the printer in the Hostname or IP address field.

9. Click Next. If the printer driver cannot be retrieved from the printer, the Install the printer driver screen appears.

10. Select the printer manufacturer and locate the model number in the Printers list box. If the printer model is not listed, click Have Disk and select the appropriate printer driver on a network drive, local hard drive, or other media.

11. Click Next to continue. The Type a printer name screen appears.

12. Accept the default printer name or type a name to identify the printer. Set this printer as the default printer if the option is available.

13. Click Next to continue. If you are using Windows 10, Windows 8.1, or Windows 7, a Printer Sharing screen appears. Select the Do not share this printer option. Click Next.

14. The printer driver installation begins. When it is finished, the final Add Printer screen appears.

15. If you want to test the printer, click Print a test page.

16. Click Finish to complete the printer installation.

Setting up a Local or Network Printer for Scheduled Reports Output

The Scheduled Reports feature allows you to send report output directly to a printer connected to or accessible with the Site Director ADS/ADX. Follow the steps in this section.

1. On the ADS/ADX computer, create a new Windows operating system user using the standard procedure specific to your particular Windows operating system.

2. Restart the computer and log in as the new user you created in Step 1.

3. Follow the steps in Setting up a Local or Network Printer on an ADS/ADX.

4. If a restart is required, log in as the new user you created in Step 1.

5. Set the printer you added in Step 3 as the default printer for the new user.

6. Print a test page to verify that printing works for the new user.

7. If the new user account has Administrator privileges, go to Step 8.
   If the new user account does not have Administrator privileges, log out and then log in with a user account that has Administrator privileges. This action enables you to perform the remaining steps in this section.


10. On the Log On tab, click This account.
11. Enter the new user’s name in the This account field and the new user’s password in the Password and Confirm password fields.

12. Click OK.

13. In the Services window, right-click Metasys III Action Queue and select Restart.

14. Test the printer by creating a scheduled report in the ADS/ADX, that is configured to go to that printer.

   ☞  **Note:** If you do not have a valid default printer set, an error message displays Print Error (263).

   Refer to the Metasys® SMP Help (LIT-1201793) for details on the Scheduled Reports feature.

### Configuring an ADS/ADX to Accept Dial-Up Connections

For an ADS/ADX to receive data via a dial-up connection from NAEs/NCEs/NIEs, each remote NAE/NCE/NIE must have its own modem and phone line connection, and each NAE/NCE/NIE and modem must be configured to dial the ADS/ADX. Refer to the Configuring an NAE to Dial Out to an ADS/ADX/ODS section in the NAE Commissioning Guide (LIT-1201519) for information on setting up an NAE/NIE to dial an ADS/ADX.

   ☞  **Note:** The ADS/ADX does not support modems on the serial port.

See Configuring Dial-Up Connections.

### Configuring Dial-Up Connections

1. Install the modem on the computer running the ADS/ADX, following the modem manufacturer’s instructions.

2. Click, or right click if using Windows 10, the Start menu or button and select Control Panel > Network and Internet > Network and Sharing Center.

3. Click Change adapter settings in the left pane. A screen showing existing network connections appears.

4. If the Menu bar is not shown, press the Alt key. A row of menu options appears on the screen.

5. Select File > New Incoming Connection. Click Continue or Yes if prompted by the User Account Control dialog. The Allow connections to this computer screen appears.

6. Select an existing user account or click Add someone to add a new user.

7. Click Next.

8. Select the correct modem to accept the incoming connections and click Next.

9. Select Internet Protocol Version 4 (TCP/IPv4) only. It does not matter if you are not able to clear other options.

10. Click Properties.

11. Clear Allow callers to access my local area network.

12. Select Specify TCP/IP addresses and type in the addresses:

   - If the NAEs using this connection are configured for Dynamic Host Configuration Protocol (DHCP), but no DHCP server exists on the network, the recommended range is
Note: The recommended IP range allows up to three simultaneous dialing connections to the ADS/ADX. Increasing the suggested range increases the number of simultaneous connections available. The IP range is not necessarily a limit on the number of modems, only the number of modems with a connected call in to the ADS/ADX.

Configure the ADS Repository attribute of the NAEs/NCEs/NIEs that dials this ADS/ADX as the first IP Address in the range of addresses chosen in this step (that is, either or 169.254.77.44 or 192.168.77.44).

13. Click **OK** to return to the wizard.

14. Click **Allow access**.

15. Click **Close** on the screen that confirms the connection has been configured.

Removing User Accounts from a Demoted Site Director

If you demote a network engine or ADS/ADX from a Site Director to a child device on the site, all user accounts that you added to the device while it was a Site Director remain in the security database. If you determine that user accounts on the demoted site should be removed after the demotion has occurred, use the SCT to perform the following steps to prepare a clean security database with all user-defined accounts deleted. This clean database can then be downloaded to the demoted device.

Changing the Site Director

Note: If you have already changed the Site Director and downloaded the site, go to Moving the Security Database and Clearing It from the Demoted Site Director.

1. Start the SCT, open the archive database for the site, and choose the new Site Director in the Site object.

2. Download the Site so that every device knows the new Site Director.

Moving the Security Database and Clearing It from the Demoted Site Director

1. Upload the archive database of the demoted device using the Manage Archive Wizard in SCT, which also backs up the Security database of the device. This step is necessary only if you are using the same set of users on the new or an existing Site Director.

2. Upload the archive database of one of the devices (ADS/ADX/network engine/SCT) on the site that has never been a Site Director and has never had a Site Director’s Security database copied to it (and, therefore, has a clean Security database with only the default user accounts).

3. Copy the Security database that you created in Step 2 to the device that was demoted from the Site Director using the Security Copy Wizard in SCT.

4. If you are using the Security database of the demoted device on the new Site Director, copy the Security database that you backed up in Step 1 to the new or existing Site Director.

5. Create a backup of the Security database from the device that was demoted and restored with a clean database in Step 3.

Note: This step ensures that the device Security database in the SCT matches the clean Security database you copied to the device in Step 3.
Configuring Metasys System Settings

The Metasys system administrator can modify default settings manually, if needed. The settings in this section reset to their default values when you upgrade the system. Reconfigure the settings as desired.

Changing Metasys Login Screen Background

You can replace the standard Johnson Controls splash screen with a custom image. For example, a customer’s name, logo, or a photo of their facility can be shown as the Site Management Portal is loading. When choosing the image, follow these recommendations:

- Use digital image files of type .jpg or .png. Avoid bitmap files, which are not compressed and often have a very large file size.
- For best results, configure the image dimensions for 800 x 600 pixels, the resolution as 96 dpi, and the color depth as 24 bit. Limit the file size to 100 KB or less. Use any photo editor, such as Microsoft Paint, to resize or reconfigure the image.
- If you use an image with a light background, you may need to change the text color for the User Name and Password fields. The default color of these fields is white and may be almost invisible over a light background.

To change the login screen background, complete the following steps:

1. Prepare the image to meet the recommendations provided at the beginning of this section.
2. Copy the image to this folder on the ADS/ADX computer: C:\Program Files (x86)\Johnson Controls\MetasysIII\UI
   Also, delete any other image files at this folder location. The only image file in this folder should be the one you want to use.
3. Open a text editor, such as Notepad, selecting the Run as Administrator option. (Highlight the text editor from the Programs list, right-click and select Run as Administrator. Specify the Administrator’s password if the operating system prompts you.) Some computers require administrator access to make changes to system files.
4. Open the FrameworkProperties.properties file on the ADS/ADX computer located here: C:\Program Files (x86)\Johnson Controls\MetasysIII\UI\com\jci\framework.
5. In the login screen background section at the end of the properties file, specify the file name of the splash screen in the loginPaneBitmapURL parameter. Be sure to remove the # character at the front of the line as shown in the following example: loginPaneBitmapURL= /<splashscreen.jpg>
6. If necessary, change the text color for the User Name and Password fields by setting the loginPaneTextColor parameter to a hexadecimal color code. Possible hex codes include: #FF0000 (red), #000000 (black), #0000FF (blue), or #FFFFFF (white). Be sure to remove the # character at the front of the line while keeping the # that precedes the hexadecimal color code, as shown in the following example (gray text): loginPaneTextColor=#808080.
8. Launch the Site Management Portal UI from the Launcher. Verify that the new background and text color appear.

Notes:
Changing the Action Queue Timeout

You may need to change this setting if you download a large number of user views or graphics that reside on a subnet different from the SCT. In this situation, the Action Queue may time out before the download is complete. The default value for the Action Queue timeout is 30 seconds.

This setting is handled in the SCT. Refer to Metasys® SCT Help (LIT-12011964) for details on changing this setting.

Creating Audit Entries for Discard Events

By default, the ADS/ADX does not create an audit entry when you discard an event that originates on the ADS/ADX.

Note: Network Engines do not create an audit entry when you discard events that originate on the engine. For details on changing this setting, refer to the NAE Commissioning Guide (LIT-1201519).

1. On the ADS/ADX computer, open Notepad.
2. Using Notepad, open the following file: C:\Inetpub\wwwroot\MetasysIII\WS\web.config
3. Find the line for WriteAuditAckDiscard:
   add key="EventRepository.WriteAuditAckDiscard" value="false"/
4. Change the value from false to true.
5. Save the file and close all windows.

Configuring Metasys Advanced Reporting System Settings

The administrator of the reporting system ADX can manually refresh data and modify default settings on the ADX such as changing the timeout period and the default number of rows allowed in a report.

The settings in this section reset to their default values when you upgrade or uninstall/reinstall the ADX software. Reconfigure the settings as desired.

Refreshing the Metasys Advanced Reporting System Data Manually

When you make changes to the SCT archive referenced by the Metasys Advanced Reporting System, the data does not refresh in the reporting system until 3:15 A.M. the following morning.

Note: Any users logged in to the reporting system at the time of the refresh are automatically logged out of the system. Perform manual refreshes at times when it is likely the system is not in use.

1. Exit the Metasys Advanced Reporting System user interface.
2. Select Start > All Programs > Accessories > Command Prompt. When you select Command
Prompt, use the right mouse key and select **Run as Administrator**. Click **Continue** or **Yes** if prompted by the User Access Control dialog.

3. Type `net stop metasysreportcacherefresh` and press **Enter**.

4. Type `net start metasysreportcacherefresh` and press **Enter**.
   - **Note:** The refresh process may take several minutes to complete. The ADX event log includes an entry when the refresh process completes, or indicates any errors.

5. Type `exit` and press **Enter**.

6. Open the Metasys Advanced Reporting System user interface, and the data reflects the changes you made to the SCT archive.

### Changing Metasys Advanced Reporting System Settings for IIS
   - **Note:** You can also change the Metasys Advanced Reporting System settings by editing the `appsettings.config` file located in the `C:\inetpub\wwwroot\MetasysReports` directory.

1. Open the **Control Panel** of the reporting system ADX and select **System and Security (or System and Maintenance) > Administrative Tools > Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) Manager window appears.

2. In the navigation tree on the left, expand the name of the local computer, Sites, and Default Web Site. The configured websites appear under the expanded Default Web Site.

3. Select the **Metasys Reports** website.

4. In the middle pane of the window, double-click **Application Settings** under the ASP.NET section. Make sure the Features View is selected. The Application Settings window appears.

5. See Table 6 to change the desired setting.

6. To edit a setting, double-click its name on the Application Settings window. Specify a new value and click **OK**.
   
### Table 6: Summary of Reporting System Changes

<table>
<thead>
<tr>
<th>Application Setting</th>
<th>Possible Edits</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Refresh</td>
<td>Edit both of the following:</td>
<td>The default time and frequency to refresh reporting system data is 3:15 A.M. and once every 24 hours. The minimum frequency is 1 hour, but is not a recommended value because any users logged in to the reporting system at the time of the refresh are automatically logged out of the system. Configure automatic refreshes to occur at times when it is likely the reporting system is not in use, and do <strong>not</strong> set frequent intervals.</td>
</tr>
<tr>
<td></td>
<td>• Edit <code>CacheRefreshBaseTime</code> to the desired refresh time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Edit <code>CacheRefreshInterval</code> to the desired number of hours between refreshes.</td>
<td></td>
</tr>
</tbody>
</table>
Table 6: Summary of Reporting System Changes

<table>
<thead>
<tr>
<th>Application Setting</th>
<th>Possible Edits</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting System User Interface Timeout</td>
<td>Edit <strong>WebServiceDBTimeout</strong> to the desired value, in seconds.</td>
<td>The <em>Metasys</em> Advanced Reporting System user interface timeout period defaults to 15 minutes (900 seconds). If the system is timing out, increase the value to 30 minutes (1800 seconds). If the system continues to time out, increase the value further. <strong>Note:</strong> The <em>Metasys</em> Advanced Reporting System user interface timeout period applies to every user who logs into the reporting system.</td>
</tr>
<tr>
<td>Report Default Row Limit</td>
<td>Edit <strong>RowsLimit</strong> to the desired value.</td>
<td>The <em>Metasys</em> Advanced Reporting System default limit for the maximum number of rows in a report is 10,000. If the report reaches or exceeds this limit, the system notifies you that the limit has been reached and the report is not generated. Increase this number to enable reports to return more than 10,000 rows of data.</td>
</tr>
</tbody>
</table>
| Default for Other Filters Panel            | Edit **MKTChecked** to one of the following:  
  • **false** if you would like the Mean Kinetic Temperature check box to be **cleared** by default.  
  • **true** if you would like the Mean Kinetic Temperature check box to be **selected** by default. | This setting determines whether Mean Kinetic Temperature is selected in the Other Filters panel. The default setting is for Mean Kinetic Temperature to be selected. |

7. When complete, close the Internet Information Services (IIS) Manager window.

8. Restart the ADX for your changes to take effect.

Changing the Archive Database Used by the *Metasys* Advanced Reporting System (Windows Server Platform Only)

**Note:** To perform this task, you must have SQL Server **CREATE PROCEDURE** permission on the archive database (to create stored procedures) and **UPDATE** permission on the *Metasys* Reporting database. As a SQL Server software administrator, you should have these permissions by default. Also, you must have Administrator rights for the Windows operating system.

This procedure is required only if you meet one of the following requirements:

• You have the *Metasys* Advanced Reporting System installed on your ADX and would like to change the archive database referenced by the reporting system without uninstalling and re-installing the ADX software.
• You have an ADX Turnkey and would like to have the reporting system refer to an archive other than MyArchive1 (the default reporting system archive database on an ADX Turnkey).

You must repeat this procedure every time you import a new database.

1. If you would like to rename your ADX computer, do so now. For a non-Turnkey system, see Appendix: Changing the ADS or ADX Name and the Computer Name on an ADS and Unified ADX. For a Turnkey system, refer to the ADS/ADX Turnkey User’s Guide (LIT-12011177).

2. Make sure the archive database you are going to associate with the reporting system is at the same release as the reporting system SCT and ADX.

3. Import the alternate archive into SCT.
   Refer to the Metasys® SMP Help (LIT-1201793) for details on importing archive databases into the SCT.

4. Select Start > All Programs > Accessories > Command Prompt. When you select Command Prompt, use the right mouse key and select Run as Administrator. Click Continue or Yes if prompted by the User Access Control dialog box.

5. Type the following at the command prompt:
   CD C:\ProgramData"Johnson Controls"\MetasysIII\SQLData\SCTArchive\ARSDBFix
   Press Enter.

6. At the prompt, type the following:
   ARSDBFix.bat “database name”
   where “database name” is the name of the alternate archive. If the name contains spaces, enclose the entire name in double quotes as in Step 5. If the name has no spaces, quotes are not required.

8. Press Enter. If errors occur during execution, they appear in the command window.
   Note: For more information on the execution, type ADRDBFix.bat /? at the prompt and press Enter.

9. At the command prompt, type the following:
   ReloadCache.bat

10. Press Enter. If errors occur during execution, they appear in the command window. When the prompt reappears, the procedure is complete.

11. Type Exit.

12. Press Enter twice.

Implementing SSL Security for the Metasys Advanced Reporting System

To implement SSL security for the Metasys Advanced Reporting System:

1. Generate a certificate request and install the certificate. For more information on these steps, see the following address: http://technet.microsoft.com/en-us/library/cc771438(WS.10).aspx.

2. Configure the Metasys software to use HTTPS (SSL) and HTTP protocols on the computer where you plan to install the reporting system.
   a. In Control Panel, select System and Security, then Administrative Tools.
b. On Administrative Tools, double-click **Internet Information Services (IIS) Manager**.

c. In the tree in the left pane, browse to and expand **Sites** or **Web Sites**.

d. In the right pane, right-click Default Web Site and select **Edit Bindings**. The Site Bindings box appears.

e. Click **Edit**. Verify that the **SSL port** field contains 443 (Figure 4).

   ☞ **Note:** Port 80 must be open on the ADX for communication from other system devices. Verify that the TCP port entry is 80.

   ![SSL Port Field: 443](image)

f. Click **OK**.

g. Close the IIS Manager window.

h. Install the ADX/ODS software with **Metasys Reporting**.

i. Using Windows Explorer, browse to: `C:\Inetpub\wwwroot\MetasysIII\UI\com\jci\framework`

j. Using a text editor, open `frameworkproperties.properties`.

k. Update the `advancedReportingURL` setting line to use **https:** instead of **http:** so it appears like the following:

   ```
   advancedReportingURL=https://SERVERNAME/MetasysReports
   ```

l. Save the file.

m. Using Windows Explorer, browse to: `C:\Inetpub\wwwroot\MetasysReports`

n. Using a text editor, open `services.config`.

o. Delete the comment tags from the file. Comment markers appear as `<!--` and `-->` (Figure 5).

   ☞ **Note:** Do not delete the text between the comment tags. Delete all three sets of comment tags that appear in the file.
Figure 5: Comment Tags

p. Save the file.
q. Close all Windows Explorer windows.
r. On the Start menu, in the Run text box, type `regedit`.
s. Click **OK**. The Registry Editor window appears.
t. In the tree on the left, browse to `HKEY_LOCAL_MACHINE > Software > Johnson Controls > Metasys > ADS`.
u. On the right side of the screen, double-click `SSRSWebURL`. The Edit String box appears.
v. In the Value data field, add an **s** after `http`. The value should be: `https://(ADx Server Name)/ReportServer` (Figure 6).

Figure 6: Edit String Box

w. Click **OK**.
x. Close the Registry Editor.

3. Restart the computer.
4. Log in to the *Metasys* Advanced Reporting System UI.
   The UI should open correctly and the URL in the browser window should have the **https** prefix.

Configuring a RADIUS Server

To configure a RADIUS account, use the Security Administrator system.
1. Using Metasys Launcher, start and log in to the SMP with any Metasys system administrator account.

2. On the SMP UI screen, select **Tools > Administrator**. The Security Administrator window appears.

3. In the **Security Administration** menu, click **RADIUS**. The Configure RADIUS screen appears.

**Figure 7: RADIUS Configure Option**
4. Select the **Enable RADIUS Authentication** check box to enable the fields on the Configure RADIUS screen.

5. Fill in the fields of the Configure RADIUS screen using the information in the following table.

**Table 7: RADIUS Configuration Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RADIUS Authentication</td>
<td>Checked or unchecked</td>
<td>Check box to configure and enable RADIUS server authentication. The check box defaults to unchecked. If it is not checked, all fields in the RADIUS Configuration screen are not editable.</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>IPv4 address or a DNS name</td>
<td>IPv4 address of the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Server Port</td>
<td>0 - 65535</td>
<td>Port on the RADIUS server to which Metasys directs messages.</td>
</tr>
</tbody>
</table>
Table 7: RADIUS Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Client Port</td>
<td>0 - 65535</td>
<td>Port on the Metasys server that is used to send requests to and receive responses from the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The default port for RADIUS is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Text string</td>
<td>A secret that is used to verify the validity of messages sent by the RADIUS server to the client. Knowing the Shared Secret does not grant access to a RADIUS server.</td>
</tr>
<tr>
<td>NAS Identifier</td>
<td>Text string</td>
<td>A RADIUS attribute that the client uses to identify itself to a RADIUS server.</td>
</tr>
<tr>
<td>Authentication Mechanism</td>
<td>MS-CHAPv2</td>
<td>Mechanism used for server authentication.</td>
</tr>
</tbody>
</table>

6. Click **Save**.

**Note:** At any time, RADIUS may be disabled by clearing the **Enable Radius Authentication** check box and applying or saving the configuration. While RADIUS is disabled, only local users can authenticate. Login errors display when a user attempts to log in with a RADIUS account.

**Adding RADIUS Users**

To provide access to the Metasys system for users that are authenticated by a RADIUS server:

1. Using Metasys Launcher, start and log in to the SMP with any Metasys system administrator account.

2. On the SMP UI screen, select **Tools > Administrator**. The Security Administration window appears.

3. Add a new RADIUS user in one of two ways:
   a. In the **Insert** Menu, click **Insert RADIUS User**.
b. Right-click the **RADIUS Users** folder. Select **Insert**.

4. The User Properties dialog box appears. Enter the User Name. **Notes:**
   - Spell out the User Name the same as defined and expected by the RADIUS server.
   - Many fields appear dimmed when you add a RADIUS user account because they are controlled by a RADIUS server. These fields include: Password, Verify Password, View Blocked Words List, View Password Policy, Min Password Length, Max Password Length, User Must Change Password at Next Logon, and User Cannot Change Password.

5. Review the selections in the remaining tabs to ensure that the appropriate **Metasys** authorization is assigned to the user. Then click **OK**. Once you add a new RADIUS user, the new user account is opened to the Access Permissions page.

   **Note:** The Maximum Password Age and Password Uniqueness fields on the Account Policy tab do not apply to RADIUS users because those features are handled by the RADIUS server.

**RADIUS Errors**

This section describes some situations that may result in error messages after enabling RADIUS to authenticate user login credentials. When the server and network engines are not configured for RADIUS authentication, the standard **Metasys** login error messages appear. When the server and network engines are configured for RADIUS authentication, RADIUS errors are intentionally obscured to hinder possible intrusion from unauthorized users. If you encounter these errors and cannot resolve them, contact your local network administrator. The two figures in this section are examples of the general RADIUS error messages.
The RADIUS error message in Figure 10 appears in any of the following scenarios:

• The RADIUS server is not online or available when the non-local (RADIUS) user tries to log in to the Metasys system.

• The server or network engine is configured to communicate with a RADIUS server, but the RADIUS server is unavailable and therefore does not respond to a login request from the non-local user.

• The non-local user's account is disabled, either in the Metasys system or in the RADIUS server.

• The non-local user's account password has expired.

• The non-local user's account password does not meet the Metasys system password complexity requirements.

• The RADIUS server is enabled, but the Metasys local user account the operator is using is disabled, locked out, or cannot log in because the user's timesheet does not permit login at this time.

• The RADIUS server is enabled, but the Metasys local user account the operator is using is entered incorrectly.

Figure 10: Login RADIUS Failure Message

The RADIUS error message in Figure 11 appears if you try to log in to a server or network engine with a non-complex password and RADIUS is not enabled.

Figure 11: Non-Complex Password Error - RADIUS Disabled

Situations When Metasys System Login Window Appears for RADIUS Users

The following situations produce the Metasys system login window for RADIUS users.

• when you log out of the Metasys Site Management Portal UI (either manually or when a user session ends)
• if RADIUS user authentication fails for any reason

• when you are logged in to the Windows OS with a RADIUS user account that is not privileged within the Metasys system

• if the RADIUS server is unavailable

• when you are logged in to the Windows OS using a local Windows account and not a RADIUS user account

• when access to RADIUS server is restricted at login time through a RADIUS user time sheet (known as Logon Hours) or access is restricted to the Metasys system through the Metasys time sheet. RADIUS server Logon Hours takes precedence, so if you are restricted from operating system access, but not restricted by a Metasys time sheet, access to the Metasys system as a RADIUS user is not granted.

• if your RADIUS user account is enabled, but overridden to disabled with the Metasys Access Suspended property within Metasys Security Administration User Properties

• if you log in to a Metasys device such as an ADS, ADX, ODS, SCT, NAE, or NCE

• if Metasys authorization fails for any reason, such as when a user without System Configuration Tool permissions attempts to log in to SCT

When the Metasys Site Management Portal UI login window appears, and the site has RADIUS authentication enabled, RADIUS appears in the Login to field. From this window, you have the following options:

• Enter a RADIUS username and password, and click RADIUS in the drop-down list.

• Enter a RADIUS username in the form of domain\username and a RADIUS password. (The Login to drop-down list becomes disabled.)

  Note: Usernames are obscured at login for RADIUS accounts. After login, usernames are partially obscured (for example, JSmith appears as JSm***).

The user credentials are strongly encrypted before being transmitted over the network for authentication. These credentials are active for the entire Metasys Site Management Portal UI session until you log out (or the user session terminates).

If the Metasys Device Manager has not fully started, and you try to log in to the ADS/ADX/ODS, a runtime status error occurs and the Metasys login window appears. In this case, the Metasys login window does not display the RADIUS server domain drop-down list and you are not able to log in as a RADIUS user.

To log in as a RADIUS user, you must close the login window, wait a few moments for the Metasys Device Manager to fully start, then navigate again to the ADS/ADX/ODS. If you remain at the login window following the startup error and do not close it, then log in with a Metasys local user account. All RADIUS menu options and functions are unavailable. To restore RADIUS options and functions, you must close the browser and navigate to the ADS/ADX/ODS again, then specify your RADIUS user credentials.

Enabling Syslog Reporting

An ADS/ADX can be set up to generate custom alarm and event email messages and send the messages to one or more specified email destinations.

1. In the Site Management Portal UI, display the ADS/ADX device object and click the Syslog tab.

2. Click Edit. The Shared Configuration section of the Syslog tab appears.
3. Click the **down** arrow for the Syslog Reporting Enabled attribute and select **True**.

4. In the Destinations section, click **New**. The Destination Configuration edit fields appear.

5. Enter the Destination Configuration values according to the following table.
   **Table 8: Attributes for Specific Syslog Destinations**
   
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Specifies a name for the Syslog server (for example, Syslog1).</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>Specifies the IP address or resolvable host name of the Syslog server that is configured to receive events and audits from the ADS/ADX/.</td>
</tr>
<tr>
<td>UDP Send Port</td>
<td>Specifies the Syslog port that is used to send messages to an ADS/ADX/.</td>
</tr>
<tr>
<td>UDP Receive Port</td>
<td>Specifies the Syslog port that is used to receive messages from an ADS/ADX/.</td>
</tr>
<tr>
<td>Event Filters</td>
<td>Specifies the rules for filtering the alarms and events that are sent to the Syslog server. Each filter has an <strong>Item</strong>, <strong>Operator</strong>, and <strong>Value</strong>.</td>
</tr>
<tr>
<td>Audit Filters</td>
<td>Specifies the rules for filtering the audit messages that are sent to the Syslog server. Each filter has an <strong>Item</strong>, <strong>Operator</strong>, and <strong>Value</strong>.</td>
</tr>
</tbody>
</table>

6. In the Event Filters section, click **New**. The Add Filter dialog box appears.

7. Select the **item**, **operator**, and **value** of the condition that you want to trigger a message to the Syslog server.

8. Add any additional event filters as desired.

9. In the Event Filters section, click **New**. The Add Filter dialog box appears.

10. Select the **item**, **operator**, and **value** of the condition that you want to trigger a message to the Syslog server.
11. Add any additional audit filters as desired.
12. Add additional Syslog destinations and filters as desired.
13. Click **OK**.
14. Click **Save**.

**Troubleshooting**

The following table includes general troubleshooting information.

Table 9: General Troubleshooting

<table>
<thead>
<tr>
<th>Error Message or Scenario</th>
<th>Solution or Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>When attempting to command a multi-state point in the <em>Metasys</em> UI, you receive the following error message: <em>The command contains values out of range, even though the values are valid.</em></td>
<td>In some instances, this error message is correct. However, occasionally the Online Archive that exists on the engine is out of sync with the Online Archive that exists on the server Site Director. To resolve this issue, execute a Sync engine command on the engine for the equipment the point resides on.</td>
</tr>
<tr>
<td>The Detail widget, Commanding dialog, or other widgets do not load completely, display partial data, or display Null as a value after installing the <em>Metasys</em> Server software and during initial startup of the <em>Metasys</em> UI.</td>
<td>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 <em>Metasys</em> UI during initial startup and sync.</td>
</tr>
<tr>
<td>On a unified <em>Metasys</em> system that is starved for resources, the ActionQueue service may not properly start at system boot. The service does run correctly if it is started after the system boot is complete.</td>
<td>Set the ActionQueue service to a delayed start.</td>
</tr>
<tr>
<td>An unsafe assembly message appears in SQL logs.</td>
<td>This message is an information message and is not an error message that requires action. This message is informing the SQL administrator that SQL cannot verify that the assembly is safe. However, the <em>Metasys</em> system uses assemblies included with <em>Metasys</em> databases to perform functions on input argument values and return data. The unsafe assembly message denotes that the assembly requires additional access to restricted resources; however, no user action is required.</td>
</tr>
</tbody>
</table>
### Table 9: General Troubleshooting

<table>
<thead>
<tr>
<th>Error Message or Scenario</th>
<th>Solution or Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>A site has multiple ADS/ADX devices, but one ADS/ADX is the Site Director and another</td>
<td>To ensure trend, alarm, or event data are forwarded to the ADS/ADX Site Director,</td>
</tr>
<tr>
<td>ADS/ADX is used as a repository. Additionally the site has multiple engines, and has</td>
<td>configure the repository ADS/ADX to forward data to the ADS/ADX Site Director.</td>
</tr>
<tr>
<td>configured a subset of engines to forward trend, alarm, or event data to the repository</td>
<td>✪ Note: This configuration is not supported for sites using the Metasys UI.</td>
</tr>
<tr>
<td>ADS/ADX instead of the ADS/ADX Site Director. This configuration may cause unexpected</td>
<td></td>
</tr>
<tr>
<td>issues if data is not forwarded from the repository ADS/ADX to the ADS/ADX Site Director.</td>
<td></td>
</tr>
<tr>
<td>For example, alarms from an engine may not appear in the ADS/ADX Site Director UI and</td>
<td></td>
</tr>
<tr>
<td>will appear in the repository ADS/ADX and the engine repository. Furthermore, if an alarm</td>
<td></td>
</tr>
<tr>
<td>is acknowledged or discarded at the repository ADS/ADX, the alarm may not be acknowledged</td>
<td></td>
</tr>
<tr>
<td>or discarded at the engine.</td>
<td></td>
</tr>
<tr>
<td>During Metasys server installation RabbitMQ configuration fails with the message:</td>
<td>Use the Administrator account when installing the Metasys Server software.</td>
</tr>
<tr>
<td>RabbitMQ.Clinet.Exceptions.</td>
<td></td>
</tr>
<tr>
<td>BrokerUnreachableException</td>
<td></td>
</tr>
<tr>
<td>RabbitMQ stops working if the hostname is changed.</td>
<td>RabbitMQ is dependent on the hostname of the machine (ADS) and if the hostname is</td>
</tr>
<tr>
<td></td>
<td>changed then the following steps are required to restart RabbitMQ:</td>
</tr>
<tr>
<td></td>
<td>1. Stop all services.</td>
</tr>
<tr>
<td></td>
<td>2. Rename the machine to the desired name.</td>
</tr>
<tr>
<td></td>
<td>3. Open a Command Prompt window with the Run as Administrator option.</td>
</tr>
<tr>
<td></td>
<td>4. In the Command Prompt window, change to this folder:</td>
</tr>
<tr>
<td></td>
<td>cd C:\ProgramFiles\RabbitMQ Server\rabbitmq_server-3.7.3\sbin.</td>
</tr>
<tr>
<td></td>
<td>5. Run: rabbitmq-service stop.</td>
</tr>
<tr>
<td></td>
<td>6. Run: rabbitmq-service remove.</td>
</tr>
<tr>
<td></td>
<td>7. Run: rabbitmq-service install.</td>
</tr>
<tr>
<td></td>
<td>8. Run: rabbitmq-service start.</td>
</tr>
<tr>
<td></td>
<td>9. Start the Metasys server installation again.</td>
</tr>
</tbody>
</table>

**Split ADX Troubleshooting**

If the web/application server needs to be restarted during runtime, you can restart the computer without any special considerations.
If the database server needs to be restarted, you must restart both the database server and the web/application server computer. The database server must be restarted before the web/application server. If you do not restart the computers in this order, the ADX application detects that the database is unavailable and enters the Warm Start sequence.

If this happens, do the following:

1. Shut down the database server.
2. Shut down the web/application server.
3. Start the database server.
4. Wait until the database server and SQL Server software are running.
5. Start the web/application server.

**ADS/ADX Slow Performance**

If the ADS/ADX encounters slow performance, the Windows indexing service or Windows log files may be contributing to the problem.

The size of the page file created by the Windows file indexing service may be as large as one gigabyte. This file size can adversely affect ADS/ADX tasks and operations. Metasys software does not require the rapid searching capability that the indexing service provides, so we recommend that you turn off indexing. To do so, open Control Panel and type Indexing in the search box. Click Indexing Options. The Indexing Options dialog box appears. Click Modify and remove all the selected locations. Click OK.

The Windows log files stored on the ADS/ADX computer may become too large, sometimes consuming gigabytes of space on the hard drive, slowing down ADS/ADX computer reboot time, system performance, and affecting database responsiveness. To correct this issue, archive all of the log files located under the following directory that are older than one week: C:\Windows \System32\Logfiles\W3SVC1. After you archive these files, delete them from the hard disk of the ADS/ADX computer. To prevent large numbers of log files in the future, you may turn off IIS event logging (also called HTTP logging) as follows:

1. In Control Panel, select System and Security > Administrative Tools > Internet Information Services (IIS) Manager.
2. Fully expand the tree and highlight Default Web Site.
3. In Features View, double-click Logging. The Logging window appears.
4. In the right pane of the Logging window, click Disable.
5. Close the Logging window.

**Note:** If you disable IIS event logging, you lose the usefulness that log files provide during troubleshooting. If you wish to troubleshoot your system, re-enable IIS event logging.

**Backup, Restoration, and Renaming of the SQL Server Databases**

Frequent backups of the SQL Server databases are necessary to maintain the integrity of your system. Examine your business needs to determine if daily, weekly, or monthly backups are necessary. The Metasys Database Manager software packaged with Metasys software provides a convenient method for database backup, restoration, and renaming. For details, refer to Metasys® Database Manager Help (LIT-12011202).

You can also perform database functions with the Microsoft SQL Server Management Studio tool. This software is included with the full editions of SQL Server software and available for the Express
editions from the Microsoft Download Center website. Contact your Johnson Controls support representative for more information on how to use third-party applications to perform backups of individual databases.

Refer to Network and IT Guidance Technical Bulletin (LIT-12011279) for more general SQL Server database recommendations.

To avoid system problems, exclude the following files and folders from any backup procedure:

- `C:\Program Files (x86)\Johnson Controls\MetasysIII`
- `C:\Program Files (x86)\Johnson Controls\MetasysIII\WS\WEB.CONFIG`
- `C:\Program Files (x86)\Johnson Controls\MetasysIII\WS\BIN`
- `C:\<WINNT or Windows>\Microsoft.NET\Framework\v1.1.4332\CONFIG`
- `C:\<WINNT or Windows>\Microsoft.NET\Framework\v2.0.50727\CONFIG`
- `C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config`
- `C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG`
- `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config`
- `C:\Program Files (x86)\Johnson Controls\MetasysIII\WS\GLOBAL.ASAX`

**Using Communication Log Files**

The Email DDA and the Pager DDA provide text-only log files to help you troubleshoot communications between the ADS/ADX and the paging terminal. The Communication Log files contain the most recent successful and unsuccessful messages sent by the DDA. If the message was unsuccessful, the log file contains a message indicating the error (for example, a pager message may have been unsuccessful due to lack of dial tone or a busy signal).

Once the log file reaches its size limit, the ADS/ADX saves the log file as a backup (.bak) file and starts with an empty log file. Once that log file reaches its size limit, the ADS/ADX again saves the log file as a backup file, this time overwriting the previous backup file.

You can open and view the log files using a text editor, such as Microsoft Notepad.

Table 10 describes the Email DDA and Pager DDA Communication Log files in the ADS/ADX. Table 11 describes the error messages that appear in the Pager DDA log file.

**Table 10: ADS/ADX Communication Log Files**

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
<th>Location of the File</th>
<th>Size Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailLog.txt</td>
<td>Displays the most recent communications between the ADS/ADX and the email recipient.</td>
<td><code>C:\ProgramData\Johnson Controls\MetasysIII</code></td>
<td>50 KB</td>
</tr>
<tr>
<td>EmailLog.bak</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PagerLog.txt</td>
<td>Displays the most recent communications between the ADS/ADX and the pager recipient.</td>
<td><code>C:\ProgramData\Johnson Controls\MetasysIII</code></td>
<td>50 KB</td>
</tr>
<tr>
<td>PagerLog.bak</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 11: Error Messages in the Pager Log File

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUSY</td>
<td>Line is busy.</td>
<td>Try sending page again.</td>
</tr>
<tr>
<td>NO ANSWER</td>
<td>Paging terminal is not answering.</td>
<td>Try sending page again.</td>
</tr>
<tr>
<td>NO CARRIER</td>
<td>Paging terminal is not answering.</td>
<td>Try sending page again.</td>
</tr>
<tr>
<td>NO DIALTONE</td>
<td>There is no dial tone heard on the phone.</td>
<td>Check the telephone cord jack.</td>
</tr>
<tr>
<td>Invalid ID</td>
<td>Pager ID is incorrect.</td>
<td>Enter a valid pager ID.</td>
</tr>
<tr>
<td>Failure to Initialize TAPI</td>
<td>• Another application is using COM port.</td>
<td>Close the other application.</td>
</tr>
<tr>
<td></td>
<td>• COM port was not closed properly.</td>
<td>Reset the NAE.</td>
</tr>
<tr>
<td></td>
<td>• COM port is busy</td>
<td>Reset the NAE.</td>
</tr>
<tr>
<td></td>
<td>• NAE Internal modem Initialization string is incorrect.</td>
<td>Change the Extra Initialization command field in the Internal Modem section of the Communications tab to M0.</td>
</tr>
</tbody>
</table>

Windows Log File Cleanup

All computers, including the ADS/ADX, generate log files related to Windows operating system functions, such as IIS. These files can accumulate and eventually cause poor computer performance since the amount of available hard disk space is reduced.

IIS logs every message it receives in C:\inetpub\logs\logfiles\w3svc1.

After consulting with your IT department, you may delete or move all IIS log files from the ADS/ADX computer to conserve hard disk space. As a precaution, you may want to retain the log files created over the past week.

In addition, several third-party tools are available to maintain your Windows operating system log files and address log file storage problems. Seek out tools that meet your needs and satisfy IT security standards on your site. Two examples of these tools are WinDirStat and CCleaner.

ADS/ADX and SCT Temporary File Cleanup

Computers with ADS/ADX and SCT software generate temporary and transient files related to the operation of the ADS/ADX and SCT. These files can accumulate and reduce the available hard disk space. You can delete or move these files offline to help save on hard disk space.

The Metasys system folders with temporary and transient files are located in C:\Users\All Users\Johnson Controls\MetasysIII.

The particular subfolders that contain temporary or transient content are:

- \Diagnostics
- \download
- \FileTransfer
- \SecurityFiles
- \temp
- \upload
When you delete or move the files under these folders, **do not** delete or move the folders themselves, just the subfolders and any files under the subfolders. Also, **do not** disturb any other MetasysIII folders that are not listed here.

**ADS/ADX Startup Failures**

See [Folders in the Windows Event Viewer on the ADS/ADX](#) for information about how these failures are logged.

If the ADS/ADX encounters an error during startup, it logs the error to the ADS/ADX Log, then enters into a Warm Start retry sequence. This sequence is the ADS/ADX trying to restart. It continues to try restarting until it is successful or until you stop the **Metasys III Device Manager** service.

If you try to stop the **Metasys III Device Manager Service** while it is in this Warm Start sequence, it could take up to 5 minutes to stop. To work around this:

1. Resolve any issue that may be causing the Startup of the ADS/ADX to fail. For example, the SQL Server software may be offline. If the issue cannot be resolved, to prevent the ADS/ADX from continually restarting, do the following:
   a. Open **Control Panel** on the ADS/ADX computer and select **Administrative Tools > Services**.
   b. In the Services window, right-click **Metasys III Device Manager** and select **Stop**.
   c. Click **OK** and close all windows.
   d. In Control Panel, select **Control Panel > System and Security > Administrative Tools > Event Viewer**.
      Service Stopped messages in the Application folder for the MIIIDM source indicate that the **Metasys III Device Manager** stopped.

      ◆ **Note:** If the **Metasys III Device Manager** is not stopped, in the **Administrative Tools > Services** window, right-click **Metasys III Device Manager** and select **Properties**. Set startup type to Manual and restart the computer. The Device Manager does not start up.

   e. The ADS/ADX **does not** start on computer restart. You must start the **Metasys III Device Manager service** manually when necessary.

2. Restart the ADS/ADX computer.

**ADS/ADX/ODS Stops Responding After Windows Updates**

This topic describes how to resolve the ADS/ADX crashing after a Windows Update.

An ADS/ADX/ODS may stop responding or may crash after Windows operating system updates are applied. After applying Windows updates to the ADS/ADX/ODS computer, we recommend restarting the computer.

On a Windows 10 computer, the ADS software may stop working after a major Windows Update. If you encounter this issue, contact your local Johnson Controls field support technician.

**Folders in the Windows Event Viewer on the ADS/ADX**

The **ADSADX Log** and **Metasys Report Server** folders in the Windows Event Viewer on the ADS/ADX contain information related to specific ADS/ADX software failures.

◆ **Note:** In a split ADX, these folders exist on the web/application server computer.
Note: Error messages appear in English only.

The following events appear in the ADSADX Log folder:

- The ADS/ADX software has a failure initializing any subsystem during startup.
- The ADS/ADX software has a failure during runtime when it tries to write to the SQL Server database.
- The ADSADX Log reports a message queue timeout has occurred. The message contains the text
  System.Messaging.Message.QueueException: Timeout for the requested operating has expired. This event indicates that MSMQ encountered an exception while reading an empty message queue. The sporadic appearance of this error in the ADSADX Log is normal. Because the error only occurs when the message queue is empty, all Metasys system messages have been processed successfully. However, if this error occurs constantly or continually over brief periods of time, there may be a problem with message queuing. Report this issue to your Johnson Controls support representative.

The ADSADX Log folder defaults to Overwrite as Necessary. If you would like to save all events or have a certain Event Log folder size, right-click the folder in the Windows Event Log and change this property.

Note: A display problem occurs when viewing the properties of the ADSADX Log in the Windows Event Viewer. Even though the folder defaults to Overwrite as Necessary when the folder is created during the first startup of the ADS/ADX, it appears in the Windows Event Viewer as Overwrite Events Older Than. In reality, the file is Overwrite as Necessary.

The Metasys Report Server folder records errors specific to the Metasys Advanced Reporting System such as:

- when a report was run
- who ran a specific report
- the destination of a report

Additional errors write to the Windows Event Viewer Application folder. Any event in this folder is a result of information generated by or an error in the Metasys III Device Manager service (MIIIDM source). Errors found in the Application folder include a connection loss between the client and server or a connection loss between the web/application server computer and database server computer in a split ADX.

To access the Windows Event Viewer Application folder:
Select Control Panel > System and Security > Administrative Tools > Event Viewer.

Anti-Spyware Software on the ADS/ADX Computer

Anti-spyware software may not allow the ADS/ADX to write to the Windows operating system Hosts file. Some anti-spyware software may prompt you to accept or reject the change; other software does not allow the change to occur at all.

If the anti-spyware software is blocking the ADS/ADX from editing the Hosts file, you can still log in to the ADS/ADX; however, you may not be able to navigate to NAEs/NCEs/NIEs or ADS/ADX devices through the ADS/ADX (Site Director) using the Metasys system user interface.

If you are using anti-spyware software, accept changes to the Hosts file that write Metasys Device Names/IP pairs to the file if you are prompted. If the software automatically denies Hosts file changes, configure the anti-spyware software to allow the IIS Admin Service to edit the Hosts file.

Configure and verify that the anti-spyware software allows the Metasys Device Manager and Metasys Action Queue services to run on the ADS/ADX computer.
**Metasys Advanced Reporting cache refresh or report execution may fail with 'Out of memory' or 'Memory pressure' messages in the SQL Server log**

When running a report with the *Metasys* Advanced Reporting system, an out of memory or memory pressure message appears in the SQL Server log. This issue only occurs on a 32-bit system that uses the /pae parameter in the boot.ini file to enable SQL Server access to more than 4 Gb memory.

Enable the Address Windowing Extensions (AWE) option. For details, refer to this Microsoft article: https://technet.microsoft.com/en-us/library/ms190961(v=sql.105).aspx

**Sync Engine Command Scenarios**

With the Sync Engine command you can synchronize the latest attributes and information available on a network engine with the Online Archive available on the Site Director. The Sync Engine command is not the same as an Archive command or an upload performed in SCT. You can only perform a Sync Engine command on an engine object in the *Metasys* UI, and that command pushes object attribute changes to the live system. An upload that you perform in SCT pushes object attributes (and other data) to the archive database, and you can view the progress of an upload in the ActionQ in SCT. Once you issue a Sync Engine command, it takes place in the background, and it is not available for monitoring. However, a flag appears on the Site object in the SMP and *Metasys* UI when an engine sync executed by a Sync Engine command is in progress.

To issue a Sync Engine command follow the steps below:

1. In the *Metasys* UI, select the engine object from the Building Network tree.
2. Tap or click on the status or value in the Detail widget. The Command dialog appears.
3. From the Command drop-down menu, select **Sync Engine**.
4. Tap or click **Save**.

The following scenarios may require a Sync Engine command:

- Data is modified directly from a network engine and not from the Site Director
- An extension is created on the live site in SMP
- A point discovery is executed on a live site in SMP

**Metasys Services Utilities Introduction**

Certain operations may require you to start or stop a service on the *Metasys* Server. These operations include, but are not limited to, the maintenance, restore, and rename functions in the *Metasys* Database Manager. Error scenarios may also require to start or stop a service on the *Metasys* Server. At *Metasys* Release 10, batch file are available for stopping, starting, and restarting the *Metasys* Server services without requiring a reboot of the host computer. When using these batch file to stop *Metasys* Server services, no data is lost because the data is sent to the appropriate queues (confirm and/or list queues).

**Metasys Services Utilities Detailed Procedures**

**Stopping the Metasys Server Services**

The batch file stops the services in a specific order:

1. **UI app pool**
2. Activity Service app pool
3. *Metasys* Activity Service
4. Event Service app pool
5. *Metasys* Event Service
6. TimeSeries app pool
7. *Metasys* TimeSeries Service
8. Scheduler Service app pool
9. *Metasys* Scheduler Service
10. Authentication Service app pool
11. *Metasys* III Device Manager Service
12. *Metasys* III Action Queue Service
13. *Metasys* app pool

To run the stop batch file from the system utilities:
1. Browse to `C:\ProgramData\Johnson Controls\MetasysIII\Diagnostics\Utilities`.
2. Right-click on the *stop.bat* and select **Run as Administrator**. Click **Yes** in the User Account Control dialog box. A Command Prompt window appears and displays the status of stopping the services. When the services stop, the Command Prompt window closes.

Starting the Metasys Server Services

The utility starts the services in a specific order:
1. *Metasys* app pool
2. *Metasys* III Action Queue Service
3. *Metasys* III Device Manager Service
4. Authentication Service app pool
5. *Metasys* Scheduler Service
6. Scheduler Service app pool
7. *Metasys* TimeSeries Service
8. TimeSeries app pool
9. *Metasys* Event Service
10. Event Service app pool
11. *Metasys* Activity Service
12. Activity Service app pool
13. UI app pool

To run the start batch file from the system utilities:
1. Browse to C:\ProgramData\Johnson Controls\MetasysIII\Diagnostics\Utilities.

2. Right-click on the start.bat and select Run as Administrator. Click Yes in the User Account Control dialog box. A Command Prompt window appears and displays the status of starting the services. When the services start, the Command Prompt window closes.

Restarting the Metasys Server Services

To run the restart batch file from the system utilities:

1. Browse to C:\ProgramData\Johnson Controls\MetasysIII\Diagnostics\Utilities.

2. Right-click on the restart.bat and select Run as Administrator. Click Yes in the User Account Control dialog box. A Command Prompt window appears and displays the status of restarting the services. When the services start, the Command Prompt window closes.

Technical Specifications

Application and Data Server (ADS) System Requirements

Table 12: Application and Data Server (ADS) System Requirements (5 Users)

<table>
<thead>
<tr>
<th>Recommended Computer Platform¹</th>
<th>Intel i7 processor latest version with at least four cores or better</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 x 500 GB hard disk (RAID 1)² with 40 GB free space after installation of all prerequisite software and before installation of ADS software. Configure RAID 1 (mirroring) with disk write-caching turned on.</td>
</tr>
<tr>
<td></td>
<td>Note: Prerequisite software includes the supported operating system, database software, .NET Framework, and any other software or service packs required for your ADS configuration.</td>
</tr>
<tr>
<td></td>
<td>Graphics card (1 GB RAM, ATI® Technologies or NVIDIA® Corporation, 64-bit compatible [for 64-bit operating systems], Small Form Factor [SFF] if required)</td>
</tr>
</tbody>
</table>

| Required Minimum Memory ² | 16 GB RAM |

<table>
<thead>
<tr>
<th>Supported Operating Systems³ and Database Software</th>
<th>Windows® 10 Pro and Enterprise Editions with Creators Update (version 1709 or later) (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports:</td>
<td>SQL Server® 2016 Express with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>SQL Server® 2014 Express with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>SQL Server® 2012 Express with SP4 (64-bit)</td>
</tr>
<tr>
<td>Note: SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/">https://support.microsoft.com/en-us/</a> kb/2979597.</td>
<td></td>
</tr>
</tbody>
</table>
| Supported Virtual Environments       | Microsoft Hyper-V™  
|                                     | VMware®          |
| Supported User Interfaces           | Site Management Portal (SMP) 
|                                     | Metasys UI       |
| Additional Software Included with the ADS Software Download | Launcher software, Network Engine images, Summary Definition Examples, Microsoft .NET Framework (multiple versions), SQL Server Management Studio, Metasys Database Manager, Toggletunnel, SNMP Management Information Base example files (MIBs), Report Viewer 2010 and Report Viewer 2012. |
| Optional Hardware                  | Any network or local printer supported by the qualified Windows operating system |
| Optional Software                  | Graphic Generation Tool 
|                                     | CCT software     
|                                     | SCT software     
|                                     | Metasys Export Utility software |

1 Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for more information regarding computer/server recommendations.
2 For best performance, use Serial Attached SCSI (SAS) hard drives, not Small Computer System Interface (SCSI) hard drives.
3 For best performance, use the maximum amount of memory that the computer allows.
4 Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for specific Microsoft Windows operating system settings that may be required for your Metasys system configuration.
### Application and Data Server-Lite System Requirements

Table 13: Application and Data Server-Lite System Requirements

| **Recommended Computer Platform** | Intel i7 processor latest version with at least 4 cores or better  
2 x 320 GB hard disk (RAID 1)\(^1\) with 40 GB free space after installation of all prerequisite software and before installation of ADS-Lite software. Configure RAID 1 (mirroring) with disk write-caching turned on.  
\(\textcircled{1}\) **Note:** Prerequisite software includes the supported operating system, database software, .NET Framework, and any other software or service packs required for your ADS configuration.  
Graphics adapter (1 GB RAM, ATI® Technologies or NVIDIA® Corporation, 64-bit compatible [for 64-bit operating systems], Small Form Factor [SFF] if required) |
| **Required Minimum Memory** | 16 GB RAM minimum |
| **Supported Operating Systems\(^2\) and Database Software** | Windows® 10 Pro and Enterprise Editions with Creators Update (version 1709 or later) (64-bit)  
Supports:  
• SQL Server® 2016 Express with SP1 (64-bit)  
• SQL Server® 2014 Express with SP2 (64-bit)  
• SQL Server® 2012 Express with SP4 (64-bit)  
\(\textcircled{1}\) **Note:** Microsoft SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to [https://support.microsoft.com/en-us/kb/2979597](https://support.microsoft.com/en-us/kb/2979597). |
|  | Windows® 8.1 Pro and Enterprise Editions with Update 1 (64-bit)  
Supports:  
• SQL Server® 2016 Express with SP1 (64-bit)  
• SQL Server® 2014 Express with SP2 (64-bit)  
• SQL Server® 2012 Express with SP3 (64-bit)  
\(\textcircled{1}\) **Note:** Microsoft SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to [https://support.microsoft.com/en-us/kb/2979597](https://support.microsoft.com/en-us/kb/2979597). |
|  | Windows® 7 Professional, Enterprise, and Ultimate Editions with SP1 (64-bit)  
Supports:  
• SQL Server® 2014 Express with SP2 (64-bit)  
• SQL Server® 2012 Express with SP3 (64-bit)  
\(\textcircled{1}\) **Note:** Microsoft SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to [https://support.microsoft.com/en-us/kb/2979597](https://support.microsoft.com/en-us/kb/2979597). |
| **Supported Virtual Environments** | Microsoft Hyper-V™  
VMware® |
Table 13: Application and Data Server-Lite System Requirements

<table>
<thead>
<tr>
<th>Supported User Interfaces</th>
<th>Site Management Portal (SMP)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Metasys UI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Software Included with the ADS-Lite Software Download</th>
<th>Microsoft SQL Server 2014 Standard SP2(^4)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft .NET Framework Version 4.6.1</td>
</tr>
<tr>
<td></td>
<td>Launcher Software</td>
</tr>
<tr>
<td></td>
<td>Metasys Database Manager software</td>
</tr>
<tr>
<td></td>
<td>Metasys Advanced Reporting System software</td>
</tr>
</tbody>
</table>

Note: The Metasys Advanced Reporting System requires an ADX. The SCT computer must be online and accessible to the ADX at all times.

<table>
<thead>
<tr>
<th>Optional Hardware</th>
<th>Any network or local printer supported by the qualified Windows operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional Software</td>
<td>Energy Essentials</td>
</tr>
<tr>
<td></td>
<td>Graphic Generation Tool</td>
</tr>
<tr>
<td></td>
<td>CCT</td>
</tr>
<tr>
<td></td>
<td>SCT</td>
</tr>
<tr>
<td></td>
<td>Metasys Export Utility</td>
</tr>
</tbody>
</table>

1. Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for more information regarding computer/server recommendations.
2. For best performance, use Serial Attached SCSI (SAS) hard drives, not Small Computer System Interface (SCSI) hard drives.
3. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for specific Microsoft Windows operating system settings that may be required for your Metasys system configuration.
4. SQL Server software is only included with the MS-ADX10SQL product.

Extended Application and Data Server System Requirements (Unified 10 or 25 User ADX)

Table 14: Extended Application and Data Server System Requirements (Unified ADX Systems, 10 or 25 Users)

<table>
<thead>
<tr>
<th>Recommended Server Platform(^1)</th>
<th>2.4 GHz Intel Xeon® 6 core single processor or better</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 x 600 GB hard disk (RAID 1)(^5) with 40 GB free space after installation of all prerequisite software and before installation of ADS software. Configure RAID 1 (mirroring) with disk write-caching turned on.</td>
</tr>
</tbody>
</table>

Note: ADX prerequisite software includes the Windows operating system, SQL Server software, Windows .NET Framework, and any other software or SPs required by your ADX configuration.

<table>
<thead>
<tr>
<th>Required Minimum Memory(^7)</th>
<th>16 to 32 GB RAM</th>
</tr>
</thead>
</table>

\(^1\) Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for more information regarding computer/server recommendations.

\(^2\) For best performance, use Serial Attached SCSI (SAS) hard drives, not Small Computer System Interface (SCSI) hard drives.

\(^3\) Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for specific Microsoft Windows operating system settings that may be required for your Metasys system configuration.

\(^4\) SQL Server software is only included with the MS-ADX10SQL product.
Table 14: Extended Application and Data Server System Requirements (Unified ADX Systems, 10 or 25 Users)

<table>
<thead>
<tr>
<th>Supported Operating Systems\ and Database Software</th>
<th>Windows® Server® 2016 (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports:</td>
<td></td>
</tr>
<tr>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>① <strong>Note:</strong> SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
<td></td>
</tr>
</tbody>
</table>

| Windows® Server® 2012 R2 with Update 1 (64-bit) |                                 |
| Supports:                                       |                                 |
| • SQL Server® 2016 with SP1 (64-bit)            |                                 |
| • SQL Server® 2014 with SP2 (64-bit)            |                                 |
| • SQL Server® 2012 with SP4 (64-bit)            |                                 |
| ① **Note:** SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to [https://support.microsoft.com/en-us/kb/2979597](https://support.microsoft.com/en-us/kb/2979597). |

| Windows® Server® 2012 (64-bit)                   |                                 |
| Supports:                                        |                                 |
| • SQL Server® 2016 with SP1 (64-bit)             |                                 |
| • SQL Server® 2014 with SP2 (64-bit)             |                                 |
| • SQL Server® 2012 with SP4 (64-bit)             |                                 |
| ① **Note:** SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to [https://support.microsoft.com/en-us/kb/2979597](https://support.microsoft.com/en-us/kb/2979597). |

| Supported Virtual Environments                  | Microsoft Hyper-V™              |
|                                                 | VMware®                         |
| Supported User Interfaces                        | Site Management Portal (SMP)     |
|                                                 | *Metasys* UI                    |
| Additional Software Included with the ADX Software Download | Microsoft SQL Server 2014 Standard SP2® |
|                                                 | Microsoft .NET Framework Version 4.6.1 |
|                                                 | Launcher Software               |
|                                                 | *Metasys* Database Manager software |
|                                                 | *Metasys* Advanced Reporting System software |
| ① **Note:** The *Metasys* Advanced Reporting System requires an ADX. The SCT computer must be online and accessible to the ADX at all times. |

| Optional Hardware                                | Any network or local printer supported by the qualified Windows operating system |
### Table 14: Extended Application and Data Server System Requirements (Unified ADX Systems, 10 or 25 Users)

<table>
<thead>
<tr>
<th>Optional Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Essentials</td>
</tr>
<tr>
<td>Graphic Generation Tool</td>
</tr>
<tr>
<td>CCT</td>
</tr>
<tr>
<td>SCT</td>
</tr>
<tr>
<td>Metasys Export Utility</td>
</tr>
</tbody>
</table>

1. Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for more information regarding computer/server recommendations.

2. For best performance, use SAS hard drives (not SATA hard drives) that use RAID controllers with write-caching enabled.

3. For best performance, use the maximum amount of memory. An ADX with 16 GB RAM has much greater performance than an ADX with only 4 GB RAM.

4. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for specific Microsoft Windows operating system settings that may be required for your Metasys system configuration.

5. SQL Server software is only included with the MS-ADX10SQL product.

For SQL Server software, you must purchase SQL Server software licenses per the guidelines listed here: SQL Server 2016, SQL Server 2014, and SQL Server 2012.

### Extended Application and Data Server System Requirements (Unified 50 or 100 User ADX)

#### Table 15: Extended Application and Data Server System Requirements (Unified ADX Systems, 50 or 100 Users)

<table>
<thead>
<tr>
<th>Recommended Server Platform¹</th>
<th>Two processors: 2.4 GHz Intel Xeon® Dual Processors with a minimum of 8 cores each or better</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6 x 300 GB 15,000 RPM hard disk (RAID 5)² with 50 GB free space after installation of all prerequisite software and before installation of ADS software. Configure RAID 5 with disk write-caching turned on.</td>
</tr>
<tr>
<td></td>
<td>RAID Controller-PERC H710 with 1 GB Cache</td>
</tr>
</tbody>
</table>

- **Note**: ADX prerequisite software includes the Windows operating system, SQL Server software, Windows .NET Framework, and any other software or SPs required by your ADX configuration.

<table>
<thead>
<tr>
<th>Required Minimum Memory</th>
<th>32 GB RAM</th>
</tr>
</thead>
</table>

ADS/ADX Commissioning Guide 57
Table 15: Extended Application and Data Server System Requirements (Unified ADX Systems, 50 or 100 Users)

<table>
<thead>
<tr>
<th>Supported Operating Systems and Database Software</th>
<th>Windows® Server® 2016 (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports:</td>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
</tr>
<tr>
<td>Note: SQL Server 2012 with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows® Server® 2012 R2 with Update 1 (64-bit)</th>
<th>Supports:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
</tr>
<tr>
<td>Note: SQL Server 2012 with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows® Server® 2012 (64-bit)</th>
<th>Supports:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
</tr>
<tr>
<td>Note: SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported Virtual Environments</th>
<th>Microsoft Hyper-V™</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware®</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported User Interfaces</th>
<th>Site Management Portal (SMP)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Metasys UI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Software Included with the ADX Software Download</th>
<th>Microsoft SQL Server 2014 Standard SP2⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft .NET Framework Version 4.6.1</td>
</tr>
<tr>
<td></td>
<td>Launcher Software</td>
</tr>
<tr>
<td></td>
<td>Metasys Database Manager software</td>
</tr>
<tr>
<td></td>
<td>Metasys Advanced Reporting System software</td>
</tr>
<tr>
<td>Note: The Metasys Advanced Reporting System requires an ADX. The SCT computer must be online and accessible to the ADX at all times.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 15: Extended Application and Data Server System Requirements (Unified ADX Systems, 50 or 100 Users)

<table>
<thead>
<tr>
<th>Optional Hardware</th>
<th>Any network or local printer supported by the qualified Windows operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional Software</td>
<td>Energy Essentials</td>
</tr>
<tr>
<td></td>
<td>Graphic Generation Tool</td>
</tr>
<tr>
<td></td>
<td>CCT</td>
</tr>
<tr>
<td></td>
<td>SCT</td>
</tr>
<tr>
<td></td>
<td>Metasys Export Utility</td>
</tr>
</tbody>
</table>

1. Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)* for more information regarding computer/server recommendations.

2. For best performance, use SAS hard drives (not SATA hard drives) that use RAID controllers with write caching enabled.

3. Refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)* for specific Microsoft Windows operating system settings that may be required for your Metasys system configuration.

4. SQL Server software is only included with the MS-ADX10SQL product. For SQL Server software, you must purchase a SQL Server software licenses per the guidelines listed here: SQL Server 2016, SQL Server 2014, and SQL Server 2012.

### Extended Application and Data Server System Requirements (Split 10 or 25 User ADX)

#### Table 16: Extended Application and Data Server System Requirements (Split ADX Systems, 10 or 25 Users)

<table>
<thead>
<tr>
<th>Recommended Server Platform¹</th>
<th>Web/Application Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.4 GHz Intel Xeon® six-core single processor or better.</td>
</tr>
<tr>
<td></td>
<td>2 x 600 GB hard disk (RAID 1)² with 40 GB free space after installation of all prerequisite software and before installation of ADS software. Configure RAID 1 (mirroring) with disk write-caching turned on.</td>
</tr>
</tbody>
</table>

**Notes:**
- *Metasys* Advanced Reporting System and Energy Essentials must reside on the ADX web/application server.
- *Metasys* UI must reside on the ADX web/application server.

<table>
<thead>
<tr>
<th>Database Server</th>
<th>2.4 GHz Intel Xeon® six core single processor or better.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 x 600 GB hard disk (RAID 1)² with 40 GB free space after installation of all prerequisite software and before installation of ADS software. Configure RAID 1 (mirroring) with disk write-caching turned on.</td>
</tr>
</tbody>
</table>

| SCT Computer                 | In a split configuration, you cannot install SCT on either the ADX web/application server computer or the ADX database server computer. Refer to the *System Configuration Tool Catalog Page (LIT-1900198)* for current SCT computer requirements. |

---

¹ For a split configuration, you cannot install SCT on either the ADX web/application server computer or the ADX database server computer. Refer to the *System Configuration Tool Catalog Page (LIT-1900198)* for current SCT computer requirements.
Table 16: Extended Application and Data Server System Requirements (Split ADX Systems, 10 or 25 Users)

<table>
<thead>
<tr>
<th>Required Minimum Memory</th>
<th>16 GB RAM (web/application server and database server for 10 or 25 user ADX)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Operating Systems³ ⁴ with Supported Database Software</td>
<td>Windows® Server® 2016 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Supports:</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> SQL Server 2012 with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
</tr>
<tr>
<td></td>
<td>Windows® Server® 2012 R2 with Update 1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Supports:</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> SQL Server 2012 with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
</tr>
<tr>
<td></td>
<td>Windows® Server® 2012 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Supports:</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2016 with SP1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2014 with SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• SQL Server® 2012 with SP4 (64-bit)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to <a href="https://support.microsoft.com/en-us/kb/2979597">https://support.microsoft.com/en-us/kb/2979597</a>.</td>
</tr>
<tr>
<td>Supported Virtual Environments</td>
<td>Microsoft Hyper-V™</td>
</tr>
<tr>
<td>Supported User Interfaces</td>
<td>VMware®</td>
</tr>
<tr>
<td>Supported User Interfaces</td>
<td>Site Management Portal (SMP)</td>
</tr>
<tr>
<td>Supported User Interfaces</td>
<td>Metasys UI</td>
</tr>
<tr>
<td>Additional Software Included with the ADX Software Download</td>
<td>Microsoft SQL Server 2014 Standard SP2⁷</td>
</tr>
<tr>
<td>Additional Software Included with the ADX Software Download</td>
<td>Microsoft .NET Framework Version 4.6.1</td>
</tr>
<tr>
<td>Additional Software Included with the ADX Software Download</td>
<td>Launcher Software</td>
</tr>
<tr>
<td>Additional Software Included with the ADX Software Download</td>
<td>Metasys Database Manager software</td>
</tr>
<tr>
<td>Additional Software Included with the ADX Software Download</td>
<td>Metasys Advanced Reporting System software</td>
</tr>
<tr>
<td><strong>Note:</strong> The Metasys Advanced Reporting System requires an ADX. The SCT computer must be online and accessible to the ADX at all times.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 16: Extended Application and Data Server System Requirements (Split ADX Systems, 10 or 25 Users)

<table>
<thead>
<tr>
<th>Optional Hardware</th>
<th>Any network or local printer supported by the qualified Windows operating system</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Optional Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Essentials</td>
</tr>
<tr>
<td>Graphic Generation Tool</td>
</tr>
<tr>
<td>CCT</td>
</tr>
<tr>
<td>SCT</td>
</tr>
<tr>
<td><em>Metasys</em> Export Utility</td>
</tr>
</tbody>
</table>

1. Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)* for more information regarding computer/server recommendations.

2. For best performance, use SAS hard drives (not SATA hard drives) that use RAID controllers with write caching enabled.

3. ADX prerequisite software includes the Windows operating system and SQL Server software, Windows .NET Framework, and any other software or service packs required for your ADX configuration.

4. For best performance, use the maximum amount of memory. An ADX with 16 GB RAM has much greater performance than an ADX with only 4 GB RAM.

5. The web/application and database servers must have the same operating system installed.

6. Refer to the *Network and IT Guidance Technical Bulletin (LIT-12011279)* for specific Microsoft Windows operating system settings that may be required for your *Metasys* system configuration.

7. SQL Server software is only included with the MS-ADX10SQL product.

For SQL Server software, you must purchase SQL Server software licenses per the guidelines listed here: [SQL Server 2016](#), [SQL Server 2014](#), and [SQL Server 2012](#).

### Extended Application and Data Server System Requirements (Split 50 or 100 User ADX)

#### Table 17: Extended Application and Data Server System Requirements (Split ADX System, 50 or 100 Users)

<table>
<thead>
<tr>
<th>Recommended Server Platform</th>
<th>Web/Application Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two processors: 2.4 GHz Intel Xeon® Dual Processors with a minimum of 8 cores each or better</td>
<td></td>
</tr>
<tr>
<td>6 x 300 GB 15,000 RPM hard disk (RAID 5) with 50 GB free space after installation of all prerequisite software and before installation of ADS software. Configure RAID 5 with disk write-caching turned on.</td>
<td></td>
</tr>
<tr>
<td>RAID Controller-PERC H710 with 1 GB cache</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- *Metasys* Advanced Reporting System and Energy Essentials must reside on the ADX web/application server.
- *Metasys* UI must reside on the ADX web/application server.
Table 17: Extended Application and Data Server System Requirements (Split ADX System, 50 or 100 Users)

<table>
<thead>
<tr>
<th><strong>Database Server</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Two processors:</strong></td>
<td>2.4 GHz Intel Xeon® Dual Processors with a minimum of 8 cores each or better</td>
</tr>
<tr>
<td>6 x 300 GB 15,000 RPM hard disk (RAID 5) with 50 GB free space after installation of all prerequisite software (^3) and before installation of ADS software. Configure RAID 5 with disk write-caching turned on.</td>
<td></td>
</tr>
<tr>
<td>RAID Controller-PERC H710 with 512 NV Cache</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SCT Computer</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>In a split configuration, you cannot install SCT on either the ADX web/application server computer or the ADX database server computer. Refer to the System Configuration Tool Catalog Page (LIT-1900198) for current SCT computer requirements.</td>
<td></td>
</tr>
</tbody>
</table>

| **Required Minimum Memory** | 32 GB RAM |
| **Supported Operating Systems and Database Software** |  |
| Windows® Server® 2016 (64-bit) | Supports: |
| • SQL Server® 2016 with SP1 (64-bit) | |
| • SQL Server® 2014 with SP2 (64-bit) | |
| • SQL Server® 2012 with SP4 (64-bit) | |
| \(\bigcirc\) **Note:** SQL Server 2012 with SP3 is not an automatic Windows update. For more information, refer to https://support.microsoft.com/en-us/kb/2979597”. |  |

| Windows® Server® 2012 R2 with Update 1 (64-bit) | Supports: |
| • SQL Server® 2016 with SP1 (64-bit) | |
| • SQL Server® 2014 with SP2 (64-bit) | |
| • SQL Server® 2012 with SP4 (64-bit) | |
| \(\bigcirc\) **Note:** SQL Server 2012 with SP3 is not an automatic Windows update. For more information, refer to https://support.microsoft.com/en-us/kb/2979597”. |  |

| Windows® Server® 2012 (64-bit) | Supports: |
| • SQL Server® 2016 with SP1 (64-bit) | |
| • SQL Server® 2014 with SP2 (64-bit) | |
| • SQL Server® 2012 with SP4 (64-bit) | |
| \(\bigcirc\) **Note:** SQL Server 2012 Express with SP3 is not an automatic Windows update. For more information, refer to https://support.microsoft.com/en-us/kb/2979597”. |  |
Table 17: Extended Application and Data Server System Requirements (Split ADX System, 50 or 100 Users)

<table>
<thead>
<tr>
<th>Supported Virtual Environments</th>
<th>Microsoft Hyper-V™</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware®</td>
</tr>
<tr>
<td>Supported User Interfaces</td>
<td>Site Management Portal (SMP)</td>
</tr>
<tr>
<td></td>
<td>Metasys UI</td>
</tr>
<tr>
<td>Additional Software Included with the ADX Software Download</td>
<td>Microsoft SQL Server 2014 Standard SP2&lt;sup&gt;7&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>Microsoft .NET Framework Version 4.6.1</td>
</tr>
<tr>
<td></td>
<td>Launcher Software</td>
</tr>
<tr>
<td></td>
<td>Metasys Database Manager software</td>
</tr>
<tr>
<td></td>
<td>Metasys Advanced Reporting System software</td>
</tr>
<tr>
<td>Note:</td>
<td>The Metasys Advanced Reporting System requires an ADX. The SCT computer must be online and accessible to the ADX at all times.</td>
</tr>
<tr>
<td>Optional Hardware</td>
<td>Any network or local printer supported by the qualified Windows operating system</td>
</tr>
<tr>
<td>Optional Software</td>
<td>Energy Essentials</td>
</tr>
<tr>
<td></td>
<td>Graphic Generation Tool</td>
</tr>
<tr>
<td></td>
<td>CCT</td>
</tr>
<tr>
<td></td>
<td>SCT</td>
</tr>
<tr>
<td></td>
<td>Metasys Export Utility</td>
</tr>
</tbody>
</table>

1 Our computer platform and memory recommendations are not meant to imply that older or slower machines are not usable. Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for more information regarding computer/server recommendations.
2 For best performance, use SAS hard drives (not SATA hard drives) that use RAID controllers with write caching enabled.
3 ADX prerequisite software includes the Windows operating system and SQL Server software, Windows .NET Framework, and any other software or service packs required for your ADX configuration.
4 For best performance, use the maximum amount of memory. An ADX with 32 GB RAM has much greater performance than an ADX with only 16 GB RAM.
5 The web/application and database servers must have the same operating system installed.
6 Refer to the Network and IT Guidance Technical Bulletin (LIT-12011279) for specific Microsoft Windows operating system settings that may be required for your Metasys system configuration.
7 SQL Server software is only included with the MS-ADX10SQL product.

For SQL Server software, you must purchase SQL Server software licenses per the guidelines listed here: SQL Server 2016, SQL Server 2014, and SQL Server 2012.

Appendix: Time Zone, Date, and Time Management

Time Zone, Date, and Time Management Introduction

The time zone, date, and time used by all devices connected to a Metasys site are synchronized automatically, preventing errors from manual time entry and clocks that become inaccurate over time. Network-wide time management ensures that scheduling, trending, audit trailing, data...
collecting, time-stamping of alarms, and other functions that require accurate time management use the same time zone, date, and time consistently for all system operations.

Time synchronization occurs on the Metasys network when an engine or server sends an IAmLive message to the Site Director. If the IAmLive message fails, the engine or server sends another message to retrieve the time from the Site Director. When the time is synchronized between the devices, a second IAmLive message is successful.

For network-wide time synchronization, the network engine/ADS/ADX/ODS designated as Site Director is the device time server because it provides the time zone, date, and time for all other engines/servers on the site. All other devices are considered time clients because they receive the time zone, date, and time from the Site Director. Beginning at Release 8.0, multiple time zone support was made available for upgraded network engines. The network engine/ADS/ADX/ODS designated as Site Director remains the device time server, but for network engines at Release 8.0 or later, the time synchronization occurs in UTC time, not in the time zone of the Site Director. For more details, see Multiple Time Zones.

To set the date and time in the Site Director (and therefore the entire site), you can set the time manually or select a time server for the Site Director. The time server for the Site Director is referred to as the site time server and should be a reliable source that is not on the Metasys network. Regardless of how you set the date and time, you must set the time zone in the Site Director.

1. **Note:** Beginning at Release 8.0, the Metasys System supports Release 8.0 (or later) network engines set in different time zones.

2. **Important:** Edit the Device Time Servers attribute or Time Sync Period attribute in the Site object only.

3. **Note:** To ensure that the correct time appears on the Site Management Portal user interface accessed from a client computer, apply the most recent Daylight Saving Time (DST) patch for the operating system on all clients that access the Site Director. The latest DST patch is available from Microsoft Corporation.

**Overview of Time Synchronization**

This section contains a summary of how time synchronizes on a site with various system components. Table 18 summarizes the time sources for various system items. All time is Universal Time Coordinated (UTC) and all system devices handle DST.

**Table 18: Time Sources**

<table>
<thead>
<tr>
<th>Item</th>
<th>Time Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAE/NIE Trend Data</td>
<td>NAE/NIE</td>
</tr>
<tr>
<td>NAE/NIE Events</td>
<td>NAE/NIE</td>
</tr>
<tr>
<td>NAE/NIE Commands</td>
<td>NAE/NIE</td>
</tr>
<tr>
<td>Annotations</td>
<td>ADS/ADX/ODS</td>
</tr>
<tr>
<td>Event Acknowledgements</td>
<td>ADS/ADX/ODS</td>
</tr>
</tbody>
</table>

**ADS/ADX/ODS Site Director with Network Engines**

On a site with an ADS/ADX/ODS Site Director and network engines, the following time synchronization steps occur:

1. ADS/ADX/ODS Site Director comes online.

2. Network engines come online and check in with the Site Director.

3. Every 15 seconds, the network engines check for ADS/ADX/ODS online/offline conditions. If the ADS/ADX/ODS is offline, the network engines send an IAmLive message to the ADS/ADX/ODS...
every 20 seconds.

4. When the ADS/ADX/ODS receives the IAmLive message, it attempts to validate the security credentials of the network engines. If the time in the network engines is different than the time in the ADS/ADX/ODS by 5 or more minutes (also taking into account the time zone of each network engine), the engine security credentials are invalidated.

5. Network engines come online and check in with the Site Director.

6. Every 15 seconds, the network engines check for ADS/ADX/ODS online/offline conditions. If the ADS/ADX/ODS is offline, the network engines send an IAmLive message to the ADS/ADX/ODS every 20 seconds.

7. When the network engine receives back an invalidated credential, the network engines request the current time from the ADS/ADX/ODS and update the engine time to match (also taking into account the time zone of each network engine).

   Note: Time between an ADS/ADX/ODS and network engines synchronizes only if the time differs between the ADS/ADX/ODS and network engines by 5 or more minutes. In the worst case scenario, one network engine could be 4 minutes and 59 seconds ahead of the ADS/ADX/ODS, and another network engine could be 4 minutes and 59 seconds behind the ADS/ADX/ODS.

8. After time is synchronized and the ADS/ADX/ODS is online, the network engines send IAmLive messages to the ADS/ADX/ODS every 5 minutes (instead of every 20 seconds).

   Note: Time synchronization is affected if you change the network engine’s Site Director from an ADS/ADX/ODS in one time zone to an ADS/ADX/ODS in a different time zone. If you make this change online, as an interim step, promote the network engine to be its own Site Director, wait several minutes, then assign to the network engine the ADS/ADX/ODS Site Director in the new time zone. This interim step ensures proper time synchronization.

NIE and Child Devices

Important: We recommend that time be synchronized carefully between the NIE and the N1 network, preferably using a common external time server. All N1 network data collected by the NIE is time stamped at the NIE (no N1 network time stamps persist in the data collected by the NIE).

While the NIE can push time to the NCM, the preferred method of synchronization for the NIE and N1 network is to have both synchronize with an external time server.

On a site with an NIE and child devices (NCMs, for example), the following time synchronization steps occur:

1. The NIE comes online and is mapped to NCMs.

2. When the time changes in the NIE (as a result of synchronization with an ADS/ADX/ODS, for example), the NIE pushes the time change down to the NCM. This time push requires that the Synchronize Time attribute of the NIE N1 Integration object is enabled.

Time Synchronization Methods

Three methods for network time synchronization are available in the Metasys system, including Windows Simple Network Time Protocol (SNTP) time synchronization, Multicast, and BACnet® time synchronization.
You can use the Microsoft Windows and Multicast methods when an SNTP master time server is available. If the Site Director has no access to SNTP time servers, you can use the BACnet synchronization method.

To enable a time synchronization method, modify the Time Sync Method attribute for the Site. See the Steps for Successful Time Management and Setting the Time Synchronization Method sections.

Windows Time Synchronization

The Windows time synchronization is Microsoft Corporation's implementation of the standard Windows SNTP w32time. This method is also referred to as unicast synchronization. With this form of time synchronization, all routers can route User Datagram Protocol (UDP) traffic. Windows time synchronization may have a larger time interval in which devices are out of sync with the SNTP master time server due to skewing and convergence.

If you use Windows time synchronization, you must define a device time server in the Site Director using the Device Time Servers attribute.

Note: If you implement an intentional time change for your site, in less than 5 minutes, all other devices on the site update with the new time with Windows time synchronization.

Multicast Time Synchronization

The Multicast time synchronization is the Johnson Controls implementation of SNTP w32time with Multicast capabilities and RFC-2030 compliance. This method delivers the same features as the Windows method, but also provides Multicast functionality. The Multicast method provides improved Metasys time synchronization between the Site Director and supervisory devices. A time server provides the master time to the Site Director, and the Site Director in turn multicasts the time to all supervisory devices on the Metasys network.

When a supervisory device first signs up with the Site Director, it polls the Site Director for the current time and matches its time with the Site Director time. By default, every 5 minutes the Site Director broadcasts the current time to all supervisory devices. If a particular device time differs 1.5 seconds or more from the Site Director time, the device adjusts its time to match. Additionally, if the Site Director time changes by more than 1 to 1.5 seconds, it sends out a Multicast time message to all devices within 2 seconds of the change.

This form of time synchronization requires that all routers on the site support Multicast routing (Internet Group Multicast Protocol [IGMP]) because the Multicast time message crosses routers. The Johnson Controls SNTP time synchronization reduces the time interval in which devices are out of sync with the SNTP master time server.

Note:

- All devices synchronized with Multicast time synchronization must be at Release 3.1 or later. For example, if you have an ADS at Release 3.1 and NAEs at Release 2.2, you cannot sync these devices using Multicast time synchronization.
- If you implement an intentional time change for your site, within a few seconds, all other devices on the site update with the new time with Multicast time synchronization.

BACnet Time Synchronization

BACnet time synchronization uses BACnet protocol to synchronize with BACnet devices such as the network engine. Use this method when the Site Director has access to a BACnet time server. This method is not available on the ADS/ADX/ODS.

Example Network

Figure 13 shows an example system with a common time zone, date, and time management setup. This example is representative of the Multicast and Windows time synchronization methods.
The ADS/ADX/ODS Site Director is configured to receive the date and time from an intranet time server. The date and time originates at an Internet time server (such as the Naval atomic clock). Using Simple Network Time Protocol (SNTP), the intranet time server requests the time from the Internet time server. The Site Director requests the time from the intranet time server. Then, using the Metasys system automatic time synchronization, and the manually configured time zone, the Site Director automatically provides the time zone, date, and time to the other engines/server on the Metasys network.

Multiple Time Zones

The time zone of the Site Director defaults to (GMT-06:00) Central Time (US & Canada). If your site is not in the Central time zone, set the time zone for your location. When you set the time zone in the Site Director, it propagates the current time to all the engines/servers on the site. You must set the time zone in the Site Director even if you select a site time server. In addition, you must set the time zone in all non-Site Director ADS/ADX/ODS devices after ADS/ADX/ODS software installation.

From Release 8.0 and later, multiple time zones across a site are supported. This functionality is set with an attribute on the network engine's Site object called Default Time Zone and the network engine's object Time Zone attribute. The Default Time Zone attribute has a drop-down list of all available world time zones to identify the local time zone where the engine is located. The operator is no longer required to apply time zone math when working with Schedule objects defined at the engine. The time zone you select is also applied to Schedule objects you define at the engine.

By default, each updated network engine continues to time-sync with the Site Director, but the time sync occurs in UTC time. For example, a Site Director in the central time zone (UTC-06:00) that syncs with an engine in the mountain time zone (UTC-07:00) does not change the engine to the central time zone. The local time and date attributes of the Site Director show its local time and date as does the network engine. Also, consider the following:

- **Scheduling:** schedules at each network engine execute relative to the local time zone of the engine, allowing you to schedule based on the local time zone, rather than the Site Director’s time zone. Prior to Release 8.0, you had to take into account the local time zone of the engine, then mentally convert the time based on the time zone of the Site Director. These time zone calculations are no longer required.

- **Historical data:** alarms, audits, and trended values from engines that are viewed on the Site Director report in local UTC time. However, alarms, audits, and trended values from engines that are viewed on the engine itself report in local time.

- **Other features:** items such as Archive Date and ADS Delivery Time report in the local time of the
The ADS/ADX/ODS Site Director and the network engines must be at Release 8.0 or later to take advantage of the multi-time zone features. If a site has a mixture of engines at different *Metasys* releases, the older engines do not exhibit this new feature. For example, as Table 19 indicates, the local time of an NAE at Release 7.0 uses the Site Director’s time, whereas an NAE at Release 8.0 or later uses a time specified by its Default Time Zone attribute.

**Table 19: Time Zone Examples**

<table>
<thead>
<tr>
<th>Device</th>
<th>Release</th>
<th>Time Zone</th>
<th>Time Zone Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS/ODS</td>
<td>8.0 or later</td>
<td>Central</td>
<td>Central Standard Time</td>
</tr>
<tr>
<td>NAE</td>
<td>6.5</td>
<td>Mountain</td>
<td>Site Director’s time zone (Central)</td>
</tr>
<tr>
<td>NAE</td>
<td>7.0</td>
<td>Central</td>
<td>Site Director’s time zone (Central)</td>
</tr>
<tr>
<td>NAE</td>
<td>8.0 or later</td>
<td>Pacific</td>
<td>Pacific Standard Time</td>
</tr>
<tr>
<td>NAE</td>
<td>8.0 or later</td>
<td>Eastern</td>
<td>Eastern Standard Time</td>
</tr>
</tbody>
</table>

**Note:** If your system consists of a network engine Site Director with multiple child network engines, make sure you use the Default Time Zone attribute of the Site object, not the Time Zone attribute in the engine, or undesirable behavior may occur.

### Site Time Server

As an alternative to setting date and time manually for a device, you can select a site time server. A site time server sets the date and time in the Site Director. If you have a split ADX, select the same site time server for both the web/application server computer and the database server computer. Site time servers can be on your intranet, such as a Domain Controller/Server; or on the Internet, such as the U.S. Naval Observatory Master Clock.


See the Selecting a Site Time Server for the Site Director Network Engine or Selecting a Site Time Server for the Site Director ADS/ADX/ODS (Windows Method Only) sections.

### Time in Device Object and User Interface Status Bar

The date, time, and time zone in the Status Bar of the SMP user interface indicates the local date, time, and time zone for that device. The date, time, and time zone in the device object to which you are browsing are the same time; however, there may sometimes seem to be a discrepancy or delay between the two. This is normal operation. See Figure 14.
For a network engine at Release 8.0 or later, the local time and date shown on the device object’s focus window is based on the default time zone set for the device. If the engine is located in a different time zone than the Site Director, the current time and date shown for each differs.

In the ADS/ADX/ODS Site Director, the time zone, date, and time in the device object of the device are set by you or by the designated site time server. In a non-Site Director network engine, the time zone, date, and time in the device object come from the Site Director. In a non-Site Director ADS/ADX, the time zone in the device object comes from your manual setting, but the date and time come from the Site Director. The device object then passes the time zone, date, and time along to the Status Bar for display. If the device is busy, it may take a few minutes for the time zone, date, and time to update correctly in the Status Bar.

**Steps for Successful Time Management**

For successful time management, do the following:

1. Verify that each non-supervisory engine/server on the Metasys network has the correct Site Director defined.  
   See the Verifying the Site Director Defined for an Engine/Server section.

2. Set the time synchronization method for the site.  
   See the Setting the Time Synchronization Method section.

3. Set the default time zone of the Site object for each network engine that has Metasys software at Release 8.0 or later.

4. Set the time zone and then set the date and time or select a site time server for the site.  
   See the Network Engine as Site Director or ADS/ADX/ODS as Site Director section.  
   If you have a network engine as the Site Director, the time zone, date, and time are set in the engine's Site object.  
   See the Network Engine as Site Director section.  
   If you have non-Site Director ADSs/ADXs on the site, you must set the time zone for these servers.  
   If you have an ADS/ADX/ODS as the Site Director, the time zone, date, and time are set in the Windows operating system of the computer where the ADS/ADX/ODS resides.  
   See the ADS/ADX/ODS as Site Director section.  
   If you have non-Site Director ADS/ADX/ODS devices on the site, you must set the time zone for these servers.

5. For Multicast time synchronization only, configure the SNTP Multicast attributes for the site.  
   See the Configuring Additional Multicast Time Synchronization Settings section.
6. If a P2000 Security Management System (SMS) is integrated to the ADS/ADX/ODS server, both
the P2000 and ADS/ADX/ODS servers should reference the same network time server. If the
two systems use different time servers, the P2000 and ADS/ADX/ODS servers are not clock
synchronized, which results in intermittent or no communication between the two systems.

Verifying the Site Director Defined for an Engine/Server

For time synchronization to work properly, all engines/servers on a site must have the correct name
for the Site Director in the Local Site Director attribute. If an engine/server has the wrong device
defined as Site Director, time synchronization may not work properly on your *Metasys* site.

1. Log in to the engine/server.
2. Drag and drop the engine/server object to the Display frame.
3. Select **Advanced**.
4. Scroll to the Site section and verify that the Local Site Director attribute contains the correct
device (Figure 15). In this example, the Site Director is a network engine (NxE-THREE).

   **Notes:**
   - The Local Site Director may be entered as an IP address or host name. If entered as
     a host name, the name is case-sensitive (for example, NxE-THREE is not the same as
     nxe-three).

   ![Figure 15: Site Director Field](image)

   - If the Site Director field contains the wrong device or is empty, click **Edit**. Edit the
     Site Director entry and click **Save**.

5. Go to **Setting the Time Synchronization Method**.

Setting the Time Synchronization Method

See the **Time Synchronization Methods** section for descriptions of the methods.

1. Log in to the Site Director engine/server.
2. Drag the Site object to the Display frame.
3. Click **Edit**.
4. Select **Advanced**.
5. In the Time section, in the Time Sync Method drop-down box, select the desired time
   synchronization method (Windows or Multicast).
6. If you select Windows time, enter a device time server in the Device Time Servers attribute. A device time server is required for Windows time synchronization.

7. Click **Save**.

   **Important:**
   When the Time Sync Method is set to Multicast and the ADS/ADX/ODS computer is synchronized with a time source other than itself, the Site Time Server must be an SNTP Time Server to allow the ADS/ADX/ODS to perform time synchronization. Time synchronization occurs when a change is detected in the ADS/ADX/ODS computer local clock, or at the Site configured Time Sync Period.

   Enabling Multicast time synchronization terminates the Windows win32time service, but changing the Time Sync Method back to Windows does not re-enable the service. If you change the Time Sync Method back to Windows, you must manually start the win32time service, or restart the Site Director.

   **Note:** When the Time Sync Method is set to Windows, also set the Internet Time Server in the Windows operating system of the Site Director to match the IP Address specified for the Site Time Server. In Control Panel of the Site Director, search for **Date and Time**. On the Date and Time dialog box, click the **Internet Time** tab. Click **Change Settings** and enter in the Server field the same IP address that you defined in the Site Time Server attribute. Click **OK** to apply the change.

8. Go to **Network Engine as Site Director** or **ADS/ADX/ODS as Site Director**.

**Network Engine as Site Director**

If a network engine is the Site Director, you must set the time zone first, then either set the date and time or select a time server for the Site Director network engine.

**Note:** See the Verifying the Site Director Defined for an Engine/Server and Setting the Time Synchronization Method sections before following the steps in this section.

**Setting the Default Time Zone in the Site Director Network Engine**

1. Log in to the Site Director network engine.

2. Drag the Site object to the Display frame.

3. Click **Edit**.
4. In the Time section, in the Default Time Zone drop-down box, select the correct time zone for the device (Figure 17).

![Figure 17: Default Time Zone in the Site Object](image)

<table>
<thead>
<tr>
<th>Time</th>
<th>(UTC-06:00) Central Time (US &amp; Canada)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Time Zone</td>
<td>(UTC-06:00) Central Time (US &amp; Canada)</td>
</tr>
<tr>
<td>Site Time Servers</td>
<td>Listof[0]</td>
</tr>
<tr>
<td>Device Time Servers</td>
<td>Listof[0]</td>
</tr>
<tr>
<td>Time SyncPeriod</td>
<td>1 hour</td>
</tr>
</tbody>
</table>

5. Click **Save**.

   **Note:** The Site object's focus window is updated immediately to indicate the current time and selected time zone, but the blue status bar in the lower right corner does not update until you log off, then log in to the network engine again.

If you are also manually setting the date and time in the Site Director network engine, go to [Setting the Date and Time in the Site Director Network Engine](#). If you are selecting a time server for the Site Director network engine, go to [Selecting a Site Time Server for the Site Director Network Engine](#).

**Setting the Date and Time in the Site Director Network Engine**

Before you manually set the date and time in the Site Director network engine, follow the steps in [Setting the Default Time Zone in the Site Director Network Engine](#).

1. In the navigation tree, right-click the Site object and select **Command**. The Command dialog box appears.

2. Click **Set Time** and enter a value in the text box (Figure 18).
3. Click **Send**.

   **Note:** If you have a site time server selected, do not attempt to set the time manually.
   If you have one or more site time servers defined, sending this command generates an error.

4. In the navigation tree, right-click the Site object and select **Command**. The Command dialog box appears.

5. Click **Set Date** and select a date from the calendar (Figure 19).
6. Click **Send**.

   - **Note:** If you have one or more site time servers defined, sending this command produces an error. If you have a site time server defined, do not attempt to set the time manually.

   The Site Director time zone, date, and time are now set and propagate to all other engines on the site.

Selecting a Site Time Server for the Site Director Network Engine

Before you select a site time server for the Site Director network engine, follow the steps in **Setting the Default Time Zone in the Site Director Network Engine**.

1. Reset the network engine for the time zone change to take effect.
2. Log in to the network engine.
3. Drag the Site object to the Display frame.
4. Click **Edit**.
5. In the Time section, in the Site Time Servers field, click the browse button.

   - **Note:** The Device Time Servers field should be blank unless you are using Windows time synchronization. Do not change the value for the Time Sync Period attribute.
6. In the screen that appears, click **Add** (Figure 20).

7. Enter the IP address of the SNTP server from which the Site Director receives its time (Figure 21).

   **Note:**
   Specify a host name only if a DNS server is available to the Site Director.

   If you add more than one address, the Site Director network engine tries to contact the first address. If that fails, the network engine contacts the second one, and so on. The network engine use only the first address in the list.

8. Click **OK**.

9. Click **Save**. The Site Director now requests the date and time from the selected time server and propagates it to all other engines on the site.

10. Go to **Configuring Additional Multicast Time Synchronization Settings**, if needed.

### ADS/ADX/ODS as Site Director

Set the time zone first, then either set the date and time or select a time server for the Site Director ADS/ADX/ODS.

**Notes:**
• See the Verifying the Site Director Defined for an Engine/Server and Setting the Time Synchronization Method sections before following the steps in this section.

• If you select a site time server for your Site Director ADS/ADX/ODS, and you also set the time manually in the ADS/ADX/ODS, the manual time is overridden at the end of the time specified in the Time Sync Period attribute (default is 1 hour).

Setting the Time Zone in the Site Director ADS/ADX/ODS

1. In the lower-right corner of the ADS/ADX/ODS computer screen, click the time. The Date and Time Properties box appears (Figure 22). The appearance of this screen varies depending on the operating system.

![Figure 22: Time and Date on a Site Director ADS/ADX/ODS](image)

2. Click Change date and time settings, then click Change time zone. The Time Zone Settings box appears.

3. Select a time zone from the drop-down list box.

4. Select Automatically adjust clock for Daylight Saving Time, if present.

5. If you have non-Site Director ADS/ADX devices on your site, set the time zone in those servers following the instructions in this section.
   If you are also manually setting the date and time in the Site Director ADS/ADX, go to the Setting the Date and Time in the Site Director ADS/ADX/ODS section.
   If you are selecting a time server for the Site Director ADS/ADX, click OK and go to the Selecting a Site Time Server for the Site Director ADS/ADX/ODS (Windows Method Only) or Selecting a Site Time Server for the Site Director ADS/ADX/ODS (Multicast Method Only) section.

Setting the Date and Time in the Site Director ADS/ADX/ODS

Before manually setting the date and time in the Site Director ADS/ADX/ODS, follow the steps in the Setting the Time Zone in the Site Director ADS/ADX/ODS section.

1. Click the time in the lower-right corner of the screen. Click Change date and time settings.

2. Set the time and date.
3. **Click OK.**
   The Site Director time zone, date, and time are now set and propagate to all other engines/servers on the site.

**Selecting a Site Time Server for the Site Director ADS/ADX/ODS (Windows Method Only)**

If you set up a site time server for your Site Director, you can set the date and time manually in the ADS/ADX/ODS, but the manual settings are overridden at the end of the Time Sync Period.

Before selecting a site time server for the Site Director ADS/ADX/ODS, follow the steps in the *Setting the Time Zone in the Site Director ADS/ADX/ODS* section.

1. On the ADS/ADX/ODS computer, press the **Windows key + R**. The Run dialog box appears (Figure 23).

![Figure 23: Run Dialog Box](image)

2. Type *Net time /setsntp:"10.10.16.1 10.10.16.2 ..."*, where 10.10.16.1 and 10.10.16.2 are example IP addresses of time servers.
   
   **Note:** The IT department should provide the address of a suitable time server. Be sure that the quotation marks are included (especially when listing multiple time servers).

3. **Click OK.**
   The Site Director now requests the date and time from the selected time server and propagates it to all other engines/servers on the site.

**Selecting a Site Time Server for the Site Director ADS/ADX/ODS (Multicast Method Only)**

Before selecting a site time server for the Site Director ADS/ADX/ODS, follow the steps in the *Setting the Time Zone in the Site Director ADS/ADX/ODS* section.

1. Log in to ADS/ADX/ODS.
2. Drag and drop the Site object to the Display frame.
3. **Click Edit.**
4. In the Time section, in the Site Time Servers field, click the **browse** button (Figure 24).
   
   **Note:** Leave the Device Time Servers field blank. Do not change the value for the Time Sync Period attribute.
5. In the screen that appears (Figure 25), click **Add**.

![Figure 25: Add Site Time Server](image)

6. Enter the IP address of the SNTP server from which the Site Director receives its time.

**Note:**
Specify a host name only if a DNS server is available to the Site Director. Leave the Device Time Servers field blank.

For Multicast time synchronization, if you add more than one address, the Site Director ADS/ADX/ODS tries to contact only the first address.

7. Click **OK**.

8. Click **Save**. The Site Director now requests the date and time from the selected time server and propagates it to all other engines/servers on the site.

9. Go to **Configuring Additional Multicast Time Synchronization Settings**.

### Configuring Additional Multicast Time Synchronization Settings

In addition to selecting the Multicast time synchronization method (**Setting the Time Synchronization Method**), you must define other Multicast attributes.

To configure additional Multicast time synchronization settings:

1. Log in to the Site Director engine/server.
2. Drag the Site object to the Display frame.

3. Click **Edit**.

4. Select **Advanced**.

5. In the Time section, modify the attributes listed in Table 20 (Figure 26).

**Figure 26: Multicast Time Synchronization Fields**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Time Zone</td>
<td><em>(UTC-06:00) Central Time (US &amp; Canada)</em></td>
</tr>
<tr>
<td>Site Time Servers</td>
<td>List of Site Time Servers</td>
</tr>
<tr>
<td>Device Time Servers</td>
<td>List of Device Time Servers</td>
</tr>
<tr>
<td>Time Sync Period</td>
<td>1 hour</td>
</tr>
<tr>
<td>Time Sync Method</td>
<td>Multicast</td>
</tr>
<tr>
<td>Multicast Group Address</td>
<td>224.0.1.1</td>
</tr>
<tr>
<td>Multicast UDP Port</td>
<td>123</td>
</tr>
<tr>
<td>Multicast TTL</td>
<td>1</td>
</tr>
<tr>
<td>Multicast Heartbeat Interval</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

Table 20: Multicast Time Synchronization Fields

- **Multicast Group Address**: Specifies the IP address used to multicast the SNTP message. This address identifies the group of devices to receive the SNTP message. The RFC-2030 defined standard address is 224.0.1.1. The address is configurable to allow site-specific use.

- **Multicast UDP Port**: Specifies the UDP port on which Multicast time synchronization polling and listens for messages. The RFC-2030 defined standard port is 123. The UDP port defined here must match the Time Server’s UDP port for successful polling to occur.

- **Multicast TTL**: Specifies the Time-to-Live (TTL) for a Multicast message. The value indicates the number of router hops allowed (number of routers to pass through) before the message is not sent. Routers must be configured to pass Multicast messages to allow the time sync message to pass.

  **Note**: A default value of 1 typically stops the Multicast message from leaving the IP subnet of the Site Director. Most routers decrease the existing TTL upon arrival of a packet, and drop the packet instead of rerouting it when the TTL reaches 0.

- **Multicast Heartbeat Interval**: Specifies the number of minutes between forcing a Multicast time synchronization message from the Site Director to participating devices.

6. Click **Save**.
Appendix: Changing the ADS or ADX Name and the Computer Name on an ADS and Unified ADX

Follow the steps in this section to change the name of an ADS/ADX. The ADS/ADX name and the computer name must match for proper functionality.

**Important:** After you follow these procedures for a Site Director, the fully qualified item references have the new ADS/ADX name and do not match the fully qualified item references in historical data. Note this detail when using tools that can access historical data, such as the Metasys Export Utility, which retrieves data representing the old item references.

**Note:** In Appendix: Changing the ODS Name and the Computer name, "ADS" or "ADS/ADX" should be read as "ODS." There are two exceptions to this, they are "ADS Repository" and "Default ADS Repository."

Overview of Changing the ADS or ADX Name and the Computer Name

This section provides an overview of the steps to change the ADS/ADX name and the computer name. You must perform all the steps referenced in this section in the correct sequence to ensure success.

**Note:** Beginning at Release 8.0, the Metasys Rename Assistant tool is included when the Metasys Database Manager is installed. This tool walks you through the rename steps outlined in this appendix in a wizard-like format. To access the Metasys Rename Assistant, browse to C:\Program Files (x86)\Johnson Controls\Metasys Database Manager. Double-click Metasys Rename Assistant in the Metasys Database Manager folder and follow the instructions on the screen. See Renaming a Computer using the Metasys Rename Assistant.

1. Prepare the computer. See Preparing the Computer.
2. Prepare the archive. See Preparing the Archive Database.
3. Uninstall the ADS/ADX and SCT software. See Uninstalling the Metasys Software.
4. Rename the computer. See Renaming the Computer.
5. Verify SQL Server software and Reporting Services functionality. See Verifying the SQL Server Software.
6. Reinstall the ADS/ADX, and SCT software and rename the Site Director. See Reinstalling the Metasys Software.
7. Download the ADS/ADX. See Downloading the Metasys Archive Database.
8. Apply the ADS/ADX settings. See Applying the ADS/ADX/ODS Settings.
9. Apply the Launcher settings. See Applying the Launcher Settings.
10. Upload your changes to the SCT. See Uploading the Metasys Archive Database.
Renaming a Computer using the *Metasys* Rename Assistant

After you rename the Site Director in SCT, use the *Metasys* Database Manager to update the Site Director and the device names in the JCI databases. Performing the rename process in both the SCT and the *Metasys* Database Manager ensures that your upgraded site can continue to access historical data.

To access the *Metasys* Rename Assistant, browse to `C:\Program Files (x86)\Johnson Controls\Metasys Database Manager`. Double-click the *Metasys* Rename Assistant in the *Metasys* Database Manager folder.

During the rename process, *Metasys* software may be uninstalled and reinstalled; refer to the installation documents when necessary. Installation documents that may be required are:

- *ADS/ADX Commissioning Guide (LIT-1201645)*
- *Energy Essentials Installation Instructions (LIT-12011539)*
- *SCT Installation and Upgrade Instructions (LIT-12012067)*

**Note:** Starting at Release 8.1, the Metasys server, SCT computer, and network engines are installed with self-signed certificates, which enables encrypted network communication between the devices. To prevent a certificate warning during a rename, the old self-signed certificate using the old computer name must be removed so that a new self-signed certificate can be generated.

Welcome

1. Once you have read the IMPORTANT notice on the screen, select the checkbox.
2. Select the **Enable SQL Server Authentication** checkbox.
3. Type your user name and password into the correct boxes.
4. Click **Test Connection**.
   **Note:**
   - If the connection is successful, **Connection: Success** appears underneath the Test Connection button and a check appears to the right of the button. If the connection fails, **Connection: Error** appears underneath the Test Connection button and an x appears to the right of the button.
   - You cannot proceed if the Test Connection was not successful.
5. Click **Get Started**.

Preparing the Computer

1. Click **Backup** to open the *Metasys* Database Manager to back up your databases. The *Metasys* Database Manager window opens.
   a. Select the **Backup** tab.
   b. Take note of the backup file path.
   c. Under Database Selection, choose which database(s) that you would like to back up.
   d. Click **Back Up Now** to back up the selected database(s).
e. Once backup is complete, close Metasys Database Manager window.

2. Select the checkbox that denotes you have performed the Metasys database backup in the Metasys Rename Assistant window.


4. Verify the time zone and time for the computer are correct, and select the checkbox denoting the Time Zone and Time are correct.
   - **Note:** If the time zone and time are not both correct, click the refresh button to update them.

5. After you have backed up the databases, uninstalled Ready Access Portal, and corrected the time zone and time, the rename box unlocks. Enter the new name that you want to assign to the ADS/ADX and click **Validate Name**.
   - **Note:**
     - The Name field is case sensitive.
     - The new name must be different from the original name.

6. Click **Continue**.
   - **Note:** A checkmark icon next to each step indicates the step is complete.

### Preparing the Archive Database

1. Click **Launch SCT** in the Metasys Rename Assistant. The Metasys Launcher opens.

2. Log in to SCT.
   - **Note:** To create a new archive, continue with Step 2. To use an archive that already exists, skip to Step 8.

3. Click **Next**. Select the **Item** menu, then select **New Archive**. The New Archive wizard opens.

4. Click **Next** in the Metasys Rename Assistant. Enter a unique name for the new archive in the box.
   - **Note:** When you are asked to close the current archive, click **Yes**.

5. Click **Next** in the Metasys Rename Assistant.
   a. Click **Create**.
   b. The Create Site window opens. Click **Yes**. The Insert Site Wizard opens.
   c. On the Destination window, select the parent item for the new item. Click **Next**.
   d. On the Identifier window, enter a unique name for the server. Click **Next**.
   e. On the Configure window, click **Next**.
      - **Note:** The order of the time zones in the Metasys software does not match the order that they are presented in in the Windows operating system. Use care to select the correct time zone from the list.

6. Click **Next** in the Metasys Rename Assistant. On the Summary window, click **Finish**. The Create
Device? window opens.

7. Click Next in the Metasys Rename Assistant. In the drop-down of the Create Device? window, select Metasys Server. Click OK. The Insert Metasys Server Wizard opens.

8. Click Next in the Metasys Rename Assistant.
   a. On the Object Type window, select the type of object that you wish to create.
   b. Click Next.
   c. On the Destination window, select the parent item for the new item.
   d. Click Next.
      † Note: If you select an item that will not work, an error message will appear.
   e. On the Identifier window, enter the original ADS/ADX name that appeared in red text in the Metasys Rename Assistant. Click Next.

9. Click Next in the Metasys Rename Assistant.
   a. On the Configure window, click Next.
   b. On the Summary window, click Finish. The Metasys Insert Site wizard closes.
   c. In SCT, select the Metasys server in the navigation tree.


11. Click Next in the Metasys Rename Assistant. On the Action screen in the Manage Archive wizard, under Type, select Upload from Device. Click Next.

12. Click Next in the Metasys Rename Assistant.
   a. On the Select Devices window, select the devices you want to upload. Click Next.
   b. On the Schedule window, click Next.

13. Click Next in the Metasys Rename Assistant.
   a. On the Site Login screen, use the computer’s name (the red text on the Metasys Rename Assistant) as the Username, and the same password you entered to log into SCT as the password for the engine.
   b. Click Test Login.
      † Note: The login process must succeed in order to proceed.

14. Click Next.
   a. On the Specify Retries window, click Next.
   b. On the Repeat Upload window, click Next.
   c. On the Summary window, click Finish. The Manage Archive wizard closes. The upload process begins. Progress is shown on the ActionQ screen in SCT.

15. Click Next in the Rename Assistant. When the completion status reports OK, right-click the
**Metasys server** in the navigation tree, click **Rename**. The Rename box appears.

16. Click **Next** in the Rename Assistant. In the new name box, enter the new ADS/ADX name written in red text in the **Metasys Rename** Assistant.

17. Click **Next** in the Rename Assistant. Click **OK**.

   ☐ **Note:**
   - If you have existing user views, open each user view in Edit mode in the SCT, use the Find/Replace function to change the name, and save the user view. The Site Director portion of the reference updates to match the new Site Director name (the name you just entered in the Rename box).
   - Do not download or make other name changes in the SCT.

18. Click **Next** in the Rename Assistant. Double-click the **Metasys site** in the navigation tree. The **Metasys** site information opens in the display pane in SCT.

19. Click **Next** in the Rename Assistant. Click **Edit** in the display pane.

20. Click **Next**.

   a. In the Name and Default ADS Repository attributes enter the name you previously entered in the Rename box. This name appears in red text in the **Metasys Rename** Assistant.

   b. Click **Save**.

21. Click **Next** in the Rename Assistant. Select **Tools > Database > Create Backup**. A notice window opens that denotes the backup is complete.

22. Click **Next** in the Rename Assistant. Exit SCT.

23. Click **Continue** in the **Metasys Rename** Assistant.

**Uninstalling the Metasys Software**

1. To uninstall **Metasys**, click the **Uninstall** button.

   ☐ **Note:**
   - A notice window opens to let you know the server is being uninstalled.
   - The installer may prompt you to take action. Click **OK** if it does.
   - You may need to restart the computer and log in.

2. Click **Continue**.

**Renaming the Computer**

1. Click **Windows Rename** in the **Metasys Rename** Assistant. The System Properties window opens.

2. Click **Next**.
a. Select the **Computer Name** tab.

b. Click **Change**. The Computer Name/Domain Changes window opens.

3. Click **Next** in the Rename Assistant. The Computer name field, enter the new ADS/ADX name. This is the red text from Rename the Computer tab of the *Metasys* Rename Assistant.

   ① **Note:**
   - If this computer is a member of a domain, specify the name in the Domain field. If the computer name includes a DNS suffix, enter the suffix.
   - If you join the computer to a domain, the DNS suffix appears automatically. If you join the computer to a workgroup, the DNS suffix is optional.

4. Click **Next** in the *Metasys* Rename Assistant. Click **OK**.

5. Click **Next** in the *Metasys* Rename Assistant. Click **OK** in the Computer Name/Domain Changes Window. The Computer Name/Domain Changes warning window opens.

   ① **Note:** You must restart your computer to apply these changes.

6. Click **Next** in the *Metasys* Rename Assistant. Close all windows.

7. Click **Next** in the *Metasys* Rename Assistant. Click **OK** when you are prompted to restart the computer. Your computer restarts.

### Verifying the SQL Server Software

1. When the SQL Server is running, click the **Reconfigure** button. When prompted, click **OK** in the Restart Computer Now window.

   ① **Note:** When you log back in to Windows, a prompt to allow the *Metasys* Rename Assistant access to your computer appears. Click **Yes**. If you are not prompted, reopen the tool manually.

2. Click the **View** button next to Report Server Web Service. The Report Server Web Service window opens

3. Select the checkbox to the left of Report Server Web Service once you have confirmed that the Report Server is working.

4. Click the **View** button next to Report Manager Site Identification URL. The Report Manager Site Identification URL window appears.

5. Check the box to the left of Report Manager Site Identification URL once you have confirmed that the Report Server is working.

6. Click **Continue**.

### Reinstalling the Metasys Software

1. Click **MDM Rename**. The *Metasys* Database Manager Window opens.

   a. Click the **Rename** tab.

   b. In the Old box, enter the **Old Site Director** name. This is found in red text in the pop-up
instructions with the *Metasys* Rename tool.

c. In the New box enter the old Site Director name, this is found in red text in the pop-up instructions with the *Metasys* Rename tool.

*Note:* Ensure you use the proper name format. The Old value should be entered as SiteDirector:SiteDirector or SiteDirector:Device. The New value should be entered as NewSiteDirector:NewSiteDirector or SiteDirector:Device.

d. Click **Rename Now**.

e. Close the *Metasys* Database Manager.

2. Click **Browse** under the Install *Metasys* SCT. The Browse window opens. Navigate to and select the **SCT installation** file. Click **Open**.

3. Click **Install**. The *Metasys* SCT installation window opens.

   a. Click **Install**.

   b. Select the server from the Server Name drop-down. Click **Install**.

   c. Click **Finish**.

4. Click **Browse** under the Install *Metasys* ADS. The Browse window opens. Navigate to and select the **ADS installation** file. Click **Open**.

5. Click **Install**. The *Metasys* Server installer opens.

   a. Click **Install**.

   b. Select the server from the Server Name drop-down. Click **Install**.

   c. Click **Restart Now**.

6. Click **Browse** under the Install Energy Essentials. The **Browse** window opens. Navigate to and select the Energy Essentials installation file. Click **Open**.

7. Click **Install**. The Energy Essentials Install window opens. Click **Install**.

8. Click **Continue**. Restart Computer Now window opens. Click **OK**.

**Downloading the Metasys Archive Database**

1. Click **Launch SCT**. The *Metasys* Launcher opens. Select SCT tab. Select **Server**. Click **Launch**. Select the archive you wish to work in.

2. Click **Next**. Open each user view in Edit mode in the SCT. Use the Find/Replace function to change the name to the new name. Save the user view. Repeat this for each user view. The Site Director portion of the reference updates to match the new Site Director name.

3. Click **Next**. Click the **Metasys server** in the navigation tree.

   *Note:* It is normal at this time for the site name to be the same as the original ADS/ADX name. Do not attempt to change the site name at this time.

4. Click **Next**. Click the **Tools** menu, then Click **Manage Archive**. The Manage Archive Wizard opens.
5. Click **Next**. On the Action window, in the Type section, Click **Download to Device**. In the Options section, select the **Include Security** checkbox so that the ADX user accounts get recreated. Click **Next**.

6. Click **Next** in the *Metasys* Rename Assistant.
   a. On the Select Devices window, select the devices to download.
   b. Click **Next**.
   c. On the Schedule window, if you need to schedule the download for a later time, select when you would like it to download.
   d. Click **Next**.
   e. On the Device Change window, click **Next**.
      
      - **Note:** Do NOT select Use this option to rename a device through the download process. Do NOT select Use this option to change a device address during the download.

7. Click **Next**.
   a. On the Site Login window, click **Test Login**.
   b. Click **Next**.
   c. Click **Next**.
   d. Click **Finish**.
   e. Close SCT.

### Applying the ADS/ADX/ODS Settings

#### ADS Settings

1. Click **Launch ADS/ADX**.
2. Click **Next**. If any user views are open, close them.
3. Click **Next**. Select the View Menu, then select **Extended Labels**.
4. Click **Next**. Double-click the *Metasys site* in the navigation tree.
5. Click **Next**. Click **Edit** in the Display pane.
6. Click **Next**. In the Name and Default ADS Repository attributes, enter the new server name.
7. Click **Next**.
   - **Note:** The name is case sensitive.
     
     In the Time Zone attribute, set the time zone to the zone written in the *Metasys Rename Assistant*.
8. Click **Next**. Click **Save**.
9. Click **Next**. Select **Refresh All Tabs** from the Action menu.
   - **Note:** The site and ADS/ADX name should now match.
10. Click **Next**. Exit the ADS/ADX Site Management Portal. The Restart Computer Now window opens.

11. Click **Next**. Click **OK**. The computer restarts.

### Applying the Launcher Settings

1. On the Desktop, right-click the **Metasys SCT** shortcut. Select **Delete**. Repeat this for the **Metasys SMP** shortcut.

2. Click **Next**.

3. Click **Launcher**.

4. Click **Next**.

   a. On the Launcher screen, click the **SMP** tab to edit an existing SMP profile.

   ⊗ **Note:** If you wish to edit a SCT profile, select the **SCT** tab instead of SMP.

   b. Log in.

5. Click **Next**.

   a. Select the profile whose description you want to edit.

   b. Click **Edit**. The Edit screen appears.

6. Click **Next**. In the New Description field, type the new name you selected for the device.

   ⊗ **Note:** You cannot change the IP address or host name of the device on the Edit screen. To make that change, delete the device, then add the device again.

7. Click **Next**. Click **Save**.

8. Click **Next**. Recreate shortcuts on the Desktop if desired.

9. Click **Continue**.

### Uploading the Metasys Archive Database

1. Launch **SCT**. Log in.

2. Click **Next**. Click the **Metasys server** in the navigation tree.

3. Click **Next**. In the Tools menu, select **Manage Archive**. The Manage Archive Wizard opens.

4. Click **Next**. In the Action window, in the Type section, select **Upload from Device**. Click **Next**.

5. Click **Next**. In the Select Devices window, select the **Metasys server** in the navigation tree. Click **Next**.

6. Click **Next**. In the Schedule window, click **Next**.

7. Click **Next**. On the Site Login window, click **Test Login**. Click **Next**.

8. Click **Next**. On the Specify Retries window, click **Next**.

9. Click **Next**. On the Repeat Upload window, click **Next**.
   - **Note:** When the upload completion status reports OK, the upload is complete. The site and server names now match.

11. Click Next. Exit the SCT.

12. Click Continue.
   - **Note:** If you are not using the Metasys Advanced Reporting System, the verification and rename processes are complete.

**Verifying the Metasys Advanced Reporting System**

1. Click Launch ADS. Log in to the ADS.
2. Click Next. Select the Tools menu, the select Metasys Advanced Reporting user interface.
3. Click Next. Log in to the Metasys Advanced Reporting user interface.
4. Click Next. Verify that the user interface appears correctly and that the site and ADX have the correct name.
5. Click Next. Verify that the navigation tree that appears in the Metasys Advanced Reporting user interfaces matches that on the SCT/ADX.
7. Click Next. Verify that the report window appears.
   - **Note:** The content of the window is not important at this time. Simply verify that the window opens successfully.
8. Click Next. Close the report window.
10. Click Next. Verify that the report window appears.
    - **Note:** The content of the window is not important at this time. Simply verify that the window opens successfully.
11. Click Next. Close the report window.
12. Click Completed. The Metasys Rename Assistant closes.

**Appendix: Configuring and Maintaining Preferences**

**Configuring and Maintaining Preferences Introduction**

The Metasys system provides customized preferences for the user interface. The preferences allow authorized users to configure how the user interface behaves, including the sounds and colors, the startup view, and the ability to add links to external applications that can be accessed from within the user interface of the ADS/ADX/ODS/SCT device.

- **Important:** Preferences do not persist after an upgrade unless you take manual steps to save the settings before you begin a system upgrade. See Preserving Preferences in an Upgrade.

Some steps in the following sections involve certain file operations, such as copying files and navigating to specific folders. The tool used for these operations is Windows File Explorer (ADS/ADX/ODS, SCT), Windows Internet Explorer®, or the Apple® Safari® web browser (). For an , log
in to the device remotely using the NxE Information and Configuration Tool (NCT), then use the Remote Desktop function in the NCT. Type **explorer** at the command prompt. For an FTP, use the Start FTP function in the NCT. Access the contents with Internet Explorer or Safari and type `ftp://<IP Address>` in the Address line. For information on the NCT, refer to the *NxE Information and Configuration Tool Technical Bulletin (LIT-1201990)*.

Preferences Concepts

System and User Preferences

Preferences are divided into two categories: **System Preferences** and **User Preferences**.

**System Preferences**

System preferences apply to all users who log in to the site or device. System preferences affect the performance and operation of the system. Only the MetasysSysAgent user and the BasicSysAgent user have authorization to configure system preferences. An audible alarm notification change is an example of a system preference. The SCT supports a subset of system preferences. If the SCT is installed on an ADS/ADX/ODS, the preferences are shared by the SMP user interface and the SCT.

Before you make system preference changes, the preferences are read from the DefaultSystemPreferences.xml file. Once you make system preference changes, a new file called SystemPreferences.xml is created (Figure 27). Both of these files are located in the directory on the Metasys system device as indicated in Table 21.

Table 21: Location of Preferences Files

<table>
<thead>
<tr>
<th>Metasys System Device</th>
<th>File Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS/ADX/ODS/SCT</td>
<td>C:\ProgramData\Johnson Controls\MetasysIII\Preferences</td>
</tr>
<tr>
<td>NAE55/NIE55</td>
<td>C:\Documents and Settings\All Users\Application Data\Johnson Controls\MetasysIII\Preferences</td>
</tr>
<tr>
<td>NAE85/NIE85</td>
<td>C:\ProgramData\Johnson Controls\MetasysIII\Preferences</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files (x86)\Johnson Controls\MetasysIII\UI\audio</td>
</tr>
<tr>
<td>NAE35/NAE45/NCE25</td>
<td>Storage\Metasys\Preferences</td>
</tr>
<tr>
<td></td>
<td>Storage\Metasys\wwwroot\metasysIII\UI\audio</td>
</tr>
</tbody>
</table>

The procedure to synchronize system preferences within a site or to reuse the system preferences on another site is a manual copy and paste process. Use the process to copy system preferences to other devices on the site or to other sites. See **Copying Preferences between Devices**.
As highlighted in Figure 27:

- **DefaultSystemPreferences.xml**: This is the default system preferences file. It is installed as part of the standard installation for all Metasys system devices.

- **SystemPreferences.xml**: This file stores the configured system preferences. If you have not yet configured system preferences, this file does not appear in the directory.

### User Preferences

User preferences apply to a specific Metasys system user. User preferences define how the information is displayed in the user interface and do not affect the operation of the system. The colors and marker styles of a trend display are examples of user preferences. Each user is authorized to view and edit their own user preferences.

The system automatically assigns a numbered user preference file name for each user called UserPreferences-userID.xml, where userID is the identification number of the user. Using an identification number, rather than using the actual user name, serves two purposes. First, it avoids any conflicts that might arise if the user name contains special characters. Second, it allows the user to be renamed without breaking the connection to the user preferences file.

To view user identification numbers, open the Security Administrator screen and select User Preference File Names under the View menu (this option is available only to the MetasysSysAgent user). The user preference file names appear in the Roles and Users pane (Figure 28) and correspond to files on the Metasys device in the directory as indicated in Table 21. As shown by two callouts in Figure 28:

- **1**: User preference file name as seen in the Security Administration in the user interface.
- **2**: User preference file as seen when accessing a network engine using Remote Desktop in the NCT.
The procedure to synchronize user preferences within a site or to reuse the user preferences on another site is a manual copy and paste process. Use the manual process to copy user preferences to other devices on the site or to other sites. See Copying Preferences between Devices.

Managing Preferences

Beginning with Metasys Server at Release 8.0, user preferences (and object lists) that are created on the ADS/ADX/ODS are saved in the archive database by SCT. They are part of the archive upload/download process, so you no longer need to save these xml files before an upgrade. However, system preferences on the ADS/ADX/ODS are not archived in SCT, so you still must manage these files manually during an upgrade.

For information on managing preferences for each preference type, see the following sections:

- System Preferences
- User Preferences
Detailed Procedures

Configuring Preferences

1. On the Tools menu of the user interface, click Configure Preferences. The Metasys Preferences dialog box appears.

2. Set the preferences according to the Preferences section of the Metasys® SMP Help (LIT-1201793). If you specified Level 1-4 Sound Files on the Alarm Settings tab, place the alarm sound files into the audio folder on the Metasys system device. The audio folder is located in the following directory:
   For ADS/ADX/ODS/NAE55/NIE55/NAE85/NIE85:
   C:\Program Files (x86)\JohnsonControls\MetasysIII\UI\audio
   For NAE35/NAE45/NCE25:
   \Storage\Metasys\wwwroot\metasysIII\UI\audio

   2. Note: If a sound file is missing from the folder, the Metasys system uses the default system beep for that alarm priority.

For Metasys UI:
   C:\Program Files (x86)\Johnson Controls\Metasys UI\Client\audio.

Restoring Default System Preferences

1. Access the Metasys system device on which you want to restore the default system preferences. (For example, if this is an , use the Remote Desktop option available in the NCT.)

2. Navigate to the Preferences directory for the device as shown in Table 21.

3. Delete the SystemPreferences.xml file.

Copying Preferences between Devices

1. Access the source Metasys system device; that is, the one that contains the preferences you want to copy. (For example, if this is an , use the Remote Desktop option available in the NCT. The local hard drive of your computer is automatically mapped to the through the remote desktop function.)

2. Navigate to the Preferences directory for the device as shown in Table 21.

3. Copy SystemPreferences.xml (system preference) or UserPreferences-userID.xml (user preference), where userID is the identification number that appears in the Security Administration tool.

4. Paste the file onto the desktop of your computer.

5. If you are accessing the Metasys system device remotely, log out.

6. Access the destination Metasys system device (where you want to copy the preferences) as the MetasysSysAgent user and navigate to the Preferences directory for the device as shown in Table 21.

7. Paste the SystemPreferences.xml file or UserPreferences-userID.xml file that you copied to your computer desktop with Step 4.
Restoring Default User Preferences

1. Log in to the SMP user interface as the MetasysSysAgent user.

2. On the Tools menu of the user interface, select **Administrator**. The Security Administration tool appears.


4. Record the file name of the user whose preferences you want to restore.

   - **Note:** If the user has been removed from the system, there is no record of the user preference file name in the Security Administration tool. In this case, remove user preference files from the **Metasys** device that do not have a corresponding user preference file name in the Security Administration tool.

5. Close the Security Administration tool and continue with **Removing User Preference Files**.

Removing User Preference Files

1. Access the **Metasys** device from which you want to remove the user preference files and navigate to the Preferences directory for the device as shown in Table 21.

2. Delete files named **UserPreferences-userID.xml**, where userID is the identification number that appears in the Security Administration tool.

   - **Note:** Do not delete DefaultUserPreferences.xml.

Copying User Preferences to Another User

1. Log in to the SMP user interface as the MetasysSysAgent user.

2. On the Tools menu of the user interface, select **Administrator**. The Security Administration tool appears.


4. Record the file name of the user whose preferences you want to copy (Source User) and the file name of the user whom you want to share those preferences (Destination User).

5. Close the Security Administration tool.

6. Access the **Metasys** device and navigate to the Preferences directory for the device as shown in Table 21.

7. Delete the preference file (if it exists) of the Destination User that you recorded in Step 4.

8. Copy and paste the user preference file of the Source User you recorded in Step 4. If using Windows File Explorer, the file appears in the folder with **Copy of** appended to the front of the file name.

9. Rename the copied file to the original name of the Destination User preference file name.

Preserving Preferences in an Upgrade

Preferences do not persist after an upgrade unless you take manual steps to save the settings before you begin a system upgrade.
1. Before you begin the upgrade process, access the Metasys server that contains the preferences and custom files you want to copy. (For example, for a network engine, use the Remote Desktop option available with NCT. The local hard drive of your computer is automatically mapped to the network engine through remote desktop.)

2. Navigate to the Preferences directory for the device as shown in Table 21.

3. Copy `SystemPreferences.xml` (system preference) or `UserPreferences-userID.xml` (user preference), where userID is the identification number for each specific user with customized preferences. If you are saving preferences for multiple users, be sure to copy all files. Also, copy any special files, such as customized sound .wav files, from the location shown in Table 21.

4. Paste these files in a safe location on your computer or network drive, or store them on other media.

5. Upgrade your system according to the *Metasys® Server Installation and Upgrade Instructions Wizard* (LIT-12012162).

6. Copy the files that you copied in Step 3 back to the appropriate location as listed in Table 21.

**Appendix: Microsoft Windows Operating System and SQL Server Software License Requirements**

**Windows Operating System License Requirements**

The Microsoft Server operating system software used by the ADX/ requires licenses called Client Access Licenses (CALs). A CAL is a license that gives you the right to access the services of the server. Two types of Microsoft operating system CALs are available: a device-based CAL and a user-based CAL. These Microsoft CALs are purchased separately from the ADX/ software as described in Purchasing and Designating CALs.

**Note:** The ADS/ running on a Windows Desktop (non-server) operating system does not require purchased operating system CALs.

**Operating System CALs**

Every site requires a combination of both device and user CALs.

**Operating System - Device CALs:** A device CAL is required for every device that accesses the ADX/ server, regardless of the number of users who access the ADX/. A device CAL is the best choice if your organization has users who access the Metasys network by sharing the same computer during their work shifts. Each NAE requires one device CAL. For example, if 15 NAEs are connected to the ADX/, a total of 15 device CALs are required. Or if 100 NAEs are connected to the ADX/, a total of 100 device CALs are required.

**Operating System - User CALs:** A user CAL is required for every user who accesses the ADX/ server, regardless of the number of computers they use for that access. A user CAL is the best choice if your organization has Metasys users who need roaming access to the Metasys network using multiple computers. For example, if two users log in to the ADX/ from different locations, two user CALs are required. Or if 10 users log in to the ADX/, 10 user CALs are required.

Another example is a security guard station. During different shifts, security guards often use a single workstation, requiring the use of only one device CAL. However, if the security guards use multiple workstations throughout the facility, one user CAL per guard is required. In this example, a single user CAL is more cost-effective, because a single ADX/ connection requires only one user CAL.
Total Number of CALs: The total number of device and user CALs required equals the total number of devices and users connected to the ADX/.

- **Example One:** If you have 100 NAEs and 10 users who use different workstations to log in, you need 110 CALs (100 device CALs and 10 user CALs).

- **Example Two:** If you have 100 NAEs and 10 users who use the same workstation to log in, you need 101 device CALs (100 device CALs for NAEs and 1 device CAL for workstation).

- **Example Three:** If you have 10 NAEs and 100 users who use different workstations to log in, you need 110 CALs (10 device CALs and 100 user CALs).

Table 22 lists the ADX/ software components and examples of what CAL combinations are required. Refer to the Metasys® System Configuration Guide (LIT-12011832) for the number of devices an ADX/ supports.

Table 22: ADX/ License and CAL Examples

<table>
<thead>
<tr>
<th>ADX/ Offering</th>
<th>Optional MVE Offering</th>
<th>Recommended Number of CALs to Purchase</th>
<th>Windows Operating System CAL Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADX10 (up to 10 users)</td>
<td>MVE5 (up to 5 users)</td>
<td>5</td>
<td>5 CALs = 2 user CALs + 3 device CALs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 CALs = 3 user CALs + 2 device CALs</td>
</tr>
<tr>
<td></td>
<td>MVE10 (up to 10 users)</td>
<td>15</td>
<td>15 CALs = 10 user CALs + 5 device CALs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15 CALs = 8 user CALs + 7 device CALs</td>
</tr>
<tr>
<td>ADXSWO (up to 25 users)</td>
<td>MVE25 (up to 25 users)</td>
<td>30</td>
<td>30 CALs = 25 user CALs + 5 device CALs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30 CALs = 10 user CALs + 20 device CALs</td>
</tr>
<tr>
<td>ADX50 (up to 50 users)</td>
<td>MVE50 (up to 50 users)</td>
<td>60</td>
<td>60 CALs = 50 user CALs + 10 device CALs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>60 CALs = 10 user CALs + 50 device CALs</td>
</tr>
<tr>
<td>ADX100 (up to 100 users)</td>
<td>None</td>
<td>110</td>
<td>110 CALs = 100 user CALs + 10 device CALs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>110 CALs = 10 user CALs + 100 device CALs</td>
</tr>
</tbody>
</table>

If you purchase Metasys system software separately from the hardware, use Table 22 to determine how many CALs you need to purchase from Microsoft. If you purchase Metasys system software as part of an ADS/ADX Ready product, the appropriate number of CALs is included in the purchase. For more details, see Purchasing and Designating CALs.

**Purchasing and Designating CALs**

You need to purchase one additional device CAL for every NAE added to your Metasys system. You may also need to purchase additional user CALs as you expand the number of authorized Metasys system users. If you currently have an ADS/ and you expand your system to require more than 10 connections, upgrade to an ADX or , you will need more CALs.
For CAL purchasing information, log in to the Johnson Controls employee portal website, go to the Tools & Applications page, then click the **Computer Price List (ADS/ADX Turnkey Info)** link in the Procurement/Purchasing section. The Computer Price List page appears. Review this page to learn how to access the Insight/Johnson Controls website (http://www.insight.com/jci) that contains information about purchasing CALs.

When you purchase CALs, you receive a paper certificate from Microsoft. There is no method in the operating system to designate or configure the number of device or user CALs. So make sure you keep the Microsoft CALs certificate in safekeeping at the customer site in case of an audit. You may be subject to a fine if a security audit reveals that your system is not correctly licensed.

If *Metasys* system software is purchased separately, the customer is responsible for purchasing the correct number of CALs and for properly designating each CAL. A device CAL cannot be transferred to a user CAL, or vice versa. If a *Metasys* Ready computer is purchased, the proper number of CALs come with the purchase, so no additional CALs are required. You must purchase additional CALs if the number of devices exceeds 5 or 10, depending on the size of the purchased *Metasys* system. Ultimately, the customer must determine how to split the total number of CALs between device and user.

For additional information on CALs, licensing, and downgrading operating system CALs, refer to [http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx](http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx).

**Licensing Modes and CAL Examples**

Figure 29 illustrates the use of CALs in a *Metasys* network.
SQL 2016, SQL Server 2014, and SQL Server 2012 Licensing Requirements

SQL Server 2016 Standard or Enterprise software, SQL Server 2014 Standard or Enterprise software and SQL Server 2012 Standard or Enterprise software use a per core licensing model. No CALs are required for SQL Server Express software.

To determine the licensing needs for SQL Server 2016, SQL Server 2014, or SQL Server 2012 software:

- count the number of cores in the processor
- purchase the adequate number of core licenses
To assist you in counting the number of processor cores, refer to the specifications provided by the computer manufacturer or download the free Microsoft Assessment and Planning Toolkit (http://www.microsoft.com/sam/en/us/map.aspx). This toolkit may require the assistance from an IT professional. You may also consult the Microsoft Core Factor Table available at http://go.microsoft.com/fwlink/?LinkID=229882.

After you determine the number of processor cores, purchase the appropriate number of core licenses to allow an unlimited number of users, NAE/NIE/NCE devices, and ADX/ computers to access the SQL Server database on that computer. If the ADX/ computer running SQL Server software has multiple cores in the processor, purchase one license for each physical core in the processor. For example, if the computer has a single quad-core processor, purchase four core licenses.

For a split ADX without the Metasys Advanced Reporting System, SQL Server software is installed only on the database server computer. You must purchase one core license for each physical core in the processor of the database server computer.

For a split ADX with the Metasys Advanced Reporting System, the database engine component of SQL Server software is present on the database server computer, and the reporting services component of SQL Server software is installed on the web/application server computer. You must purchase one core license for each physical core in the processor for both the database server computer and the web/application server computer.

Table 23 lists the number of core licenses required based on the number of physical cores in the processor.

Table 23: SQL Server 2014 or SQL Server 2012 License Requirements

<table>
<thead>
<tr>
<th>Physical Cores in the Processor</th>
<th>Core Licenses Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(SQL Server 2016, SQL Server 2014, or SQL Server 2012 software requires a minimum of four core licenses, even for processors with less than four cores.)</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

**ADS/ADS-Lite or Requirements**

The ADS/ADS-Lite or software does not come with, and does not require, device or user CALs. Also, the ADS/ADS-Lite or uses the free version of SQL Server Express software, so you do not need to purchase SQL Server CALs.

To avoid ADS/ADS-Lite or connection and network communication performance issues, the number of users and the number of NAE/NIE/NCE devices and ADS/ADS-Lite or computers that transfer trend data, event messages, and audit messages should not exceed 10. If a Metasys site with a single ADS/ADS-Lite configured as the Site Director and default repository exceeds that number of connections, consider one of the following options:

- Configure one ADS/ADS-Lite or to be the Site Director. Install and configure another ADS/ADS-Lite or (or more) to provide the ADS repository function. When you install a separate ADS or ADS-Lite or to provide the repository function, it allows you to dedicate five connections on the alternate ADS or for system users and another five connections on the alternate ADS/ADS-Lite or to NAE/ NIE/NCE devices and ADS/ADS-Lite/ computers for transferring trend data, event messages, or audit messages.
Note: The ADS/ADS-Lite or cannot be the Site Director for another ADS/ADS-Lite/ of any type.

- Upgrade to an ADX or . Configure the Windows Server of the ADX/ computer with the number of CALs equal to the total number of users and devices accessing the ADX/. In addition, configure the SQL Server database with one SQL Server Processor license.

Refer to the *Metasys® System Configuration Guide (LIT-12011832)* for performance guidelines and limitations.

**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.

**Opening Ports Configuring the 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.

This section provides an overview on how to open ports to make sure *Metasys* software and processes function properly. At Release 8.1 and later, you can create rules to block inbound and outbound traffic over Port 80 (http). For details, see Closing Ports.

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.
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 (80, 88, 123, 135, 389, 443, 445, 1025, 1433, 9910, 15672, 5672, 36672, 4369, 9200, and 5601) as shown in 15.

### Table 24: Ports to Open for TCP Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
</tr>
<tr>
<td>Kerberos</td>
<td>88</td>
<td>TCP</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC)</td>
<td>135</td>
<td>TCP</td>
</tr>
<tr>
<td>LDAP</td>
<td>389</td>
<td>TCP</td>
</tr>
<tr>
<td>Secure Sockets Layer (SSL)</td>
<td>443</td>
<td>TCP</td>
</tr>
<tr>
<td>NT LAN Manager Version 2 (NTLMv2)</td>
<td>445</td>
<td>TCP</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC)</td>
<td>1025</td>
<td>TCP</td>
</tr>
<tr>
<td>Microsoft SQL Server Database</td>
<td>1433</td>
<td>TCP</td>
</tr>
<tr>
<td>Microsoft Discovery Protocol</td>
<td>9910</td>
<td>TCP</td>
</tr>
<tr>
<td>HTTP for RabbitMQ</td>
<td>15672</td>
<td>TCP</td>
</tr>
<tr>
<td>AMQP for RabbitMQ</td>
<td>5672</td>
<td>TCP</td>
</tr>
<tr>
<td>EPMD for RabbitMQ</td>
<td>25672</td>
<td>TCP</td>
</tr>
<tr>
<td>EPMD for Erlang Port Mapper Daemon, RabbitMQ</td>
<td>4369</td>
<td>TCP</td>
</tr>
<tr>
<td>HTTP for Elasticsearch</td>
<td>9200</td>
<td>TCP</td>
</tr>
<tr>
<td>HTTP for Kibana</td>
<td>5601</td>
<td>TCP</td>
</tr>
</tbody>
</table>
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 80, 88, 135, 389, 443, 445, 1025, 1433, and 9910 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, 161, 162, 9910, 9911, 47808).

   **Table 25: Ports to Open for UDP Protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>25</td>
<td>UDP</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP</td>
</tr>
<tr>
<td>DHCP</td>
<td>67</td>
<td>UDP</td>
</tr>
<tr>
<td>DHCP</td>
<td>68</td>
<td>UDP</td>
</tr>
<tr>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>69</td>
<td>UDP</td>
</tr>
<tr>
<td>Kerberos</td>
<td>88</td>
<td>UDP</td>
</tr>
<tr>
<td>Network Time Protocol (NTP)</td>
<td>123</td>
<td>UDP</td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
<td>UDP</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>162</td>
<td>UDP</td>
</tr>
<tr>
<td>Microsoft Discovery Protocol</td>
<td>9910</td>
<td>UDP</td>
</tr>
<tr>
<td>SYPE-Transport</td>
<td>9911</td>
<td>UDP</td>
</tr>
<tr>
<td>BACnet®</td>
<td>47808</td>
<td>UDP</td>
</tr>
</tbody>
</table>

   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.
15. Close the **Windows Firewall with Advanced Security** window.

16. Close all windows.

**Closing Ports**

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.

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** 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 wish 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)*.
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)*. 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**.


**Appendix: Installing Antivirus Software**

Follow the steps in this appendix for installing antivirus software on computers that run ADS/ADX or SCT software. We recommend one of the following antivirus software programs:

- Symantec® Endpoint Protection software Corporate Edition version 12.0 or later
- McAfee® VirusScan® Enterprise version 8.8 with Patch 9

**Note:** Windows Defender, provided by some Microsoft operating systems, **is not** supported on a computer that is running ADS/ADX or SCT software. Make sure you turn off Windows Defender before bringing the system online.

**Installing and Configuring Symantec® Endpoint Protection Software**

Symantec Endpoint Protection software at version 12.0 or later is permitted on computers that run ADS/ADX or SCT software. You may install Symantec Endpoint Protection software on a **Metasys** system in a unified, split, or virtual machine configuration.

You can use any release of SEP version 12.0 on your Windows 7. For Windows 10, Windows 8.1, Windows Server 2012 R2, or Windows Server 2012, use SEP version 12.1.2 or 12.1 RU2 or higher. However, within the SEP software configuration, select only the anti-virus and anti-spyware features. The other two features, **Proactive Threat Protection** and **Network Threat Protection**, can interfere with communication between Metasys software and supervisory devices. Follow the steps in this section to properly install and configure this software.

During and after installation of the Symantec Endpoint Protection software on the **Metasys system**, we recommend the following settings and best practices:
• Select **Install an unmanaged client**. A question box appears regarding installation as an unmanaged client. Click **Yes** to continue.

• The Symantec Endpoint Protection software at version 14.0 installation wizard no longer has the option to install an unmanaged client. To do so with this version of software, refer to Symantec's proprietary support here: [https://support.symantec.com/en_US/article.HOWTO101759.html](https://support.symantec.com/en_US/article.HOWTO101759.html).

• Select **Unmanaged client** for the Client Type.
  
  **Note:** Do not select **Managed client**. If your network is managed by a Symantec server, selecting the Managed Client option changes the custom settings and could prevent the Metasys user interface from working correctly.

• Select the **Custom** setup type.

• Disable the installation of these options: Advanced Download Protection, Outlook Scanner, Notes Scanner, POP3/SMTP Scanner, Proactive Threat Protection, and Network Threat Protection. To disable, click the **down arrow** and select **Entire feature will be unavailable**.

• Select **Enable Auto-Protect**, **Run LiveUpdate**, and **Disable Windows Defender** (if the option is available) for Protection Options.

• Do not select the File Reputation Data Submission check box.

• Do not select the check box under Data Collection -- Installation Options.

• Allow the LiveUpdate process to complete after installation of the Symantec Endpoint Protection software.

• Double-click the **Symantec Endpoint Protection** icon in the Windows task bar. The Status screen appears. Verify that the Proactive Threat Protection and Network Threat Protection features are not installed. If they do not appear on the Status screen, they are not installed.

• If the Proactive Threat Protection and Network Threat Protection features are installed, they appear on the Status screen. You must remove them from your computer.

  a. In Control Panel, select **Programs > Programs and Features**. Click **Symantec Endpoint Protection** in the list of installed programs.

  b. Click **Change** to start the InstallShield Wizard for Symantec Endpoint Protection.

  c. When you reach the Program Maintenance screen, select **Modify**. Click **Next**. The Custom Setup screen appears.

  d. Click the feature icon and select **Entire feature will be unavailable** for both Proactive Threat Protection and Network Threat Protection. An X appears in front of those features. Click **Next**. Complete the steps in the installation wizard.

### Installing and Configuring McAfee VirusScan Enterprise Software

McAfee® VirusScan® Enterprise version 8.8 with Patch 9 is permitted on computers that run ADS/ADX or SCT software. You may install McAfee anti-virus software on a Metasys system in a unified, split, or virtual machine configuration.

We recommend installing McAfee VirusScan Enterprise software using the steps in McAfee VirusScan Enterprise Installation. If you deviate from these steps, Metasys software may not work
correctly. If you must enable higher security settings from what is recommended, gradually add changes and check for system reliability as you do so.

During and after installation of the McAfee VirusScan Enterprise software on the Metasys system, we recommend the following settings and best practices:

1. Select the **Typical** or **Custom** setup type.
2. Select **Standard Protection** for the Access Protection Level.
3. Select **Run On-Demand Scan** when the installation is complete. We recommend that you take the time now to run a full scan to ensure the computer is prepared for Metasys software. This process can take from 30 to 60 minutes to complete.

Once the installation is complete, configure McAfee as follows:

1. Open the **VirusScan Console**, click **Task > Properties**. The Access Protection Properties window appears. Under Categories, select **Anti-virus Standard Protection**. In the protection rules table, remove the **Block and Report** check marks for **Prevent Mass Mailing Worms From Sending Mail**. Leave all other category settings at their defaults.
2. Right-click **Full Scan** in the VirusScan Console, and select Properties.
3. Click the **Performance** tab. Under System utilization, slide the bar pointer to the **Low** setting.
4. Click **Schedule**, and with the assistance of your local IT staff, define a daily scan schedule. Do not scan at midnight because the Metasys system performs a daily archive at that time.
5. Click OK to save the schedule. Click OK on the On-Demand Scan Properties-Full Scan window.
7. Click the **All Processes** icon, then select **Configure** different scanning policies for high-risk, low-risk, and default processes. The left pane refreshes to show additional icons.
8. Click **Low-Risk Processes**.
9. Click **Add** and add Sqlservr.exe and Sqlwriter.exe to the list of low-risk processes. (If the files do not appear in the list box, click **Browse** and locate them under the Microsoft SQL Server folder.)
10. Click OK to save the changes.

**Note:** RabbitMQ is a dependancy of ADS/ADX and requires ports 15672, 5672, 25672, and 4369 to work. McAfee blocks these ports by default so they must be added into the antivirus firewall.

### Related Documentation

Table 26: ADS/ADX Commissioning Related Documentation

<table>
<thead>
<tr>
<th>For Information On</th>
<th>See Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Object Configuration and the Metasys System User Interface</td>
<td>Metasys® SMP Help (LIT-1201793)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This LIT number represents a print-friendly version of the Help.</td>
</tr>
<tr>
<td>For Information On</td>
<td>See Document</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ADS/ADX Features and Benefits</td>
<td>Application and Data Server (ADS) and Extended Application and Data Server (ADX) Product Bulletin (LIT-1201525)</td>
</tr>
<tr>
<td>Installation and Upgrade of ADS/ADX Software</td>
<td>SCT Installation and Upgrade Instructions (LIT-12012067); Metasys® Server Installation and Upgrade Instructions (LIT-12012162)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use the wizard to generate instructions specific to your system.</td>
</tr>
<tr>
<td>Installation and Upgrade of ADS-Lite Software</td>
<td>ADS-Lite Installation and Upgrade Instructions Wizard (LIT-12011688)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use the wizard to generate instructions specific to your system.</td>
</tr>
<tr>
<td>License Information</td>
<td>Metasys System Extended Architecture License Information Part No. 24-10067-1</td>
</tr>
<tr>
<td>Metasys System (General)</td>
<td>Metasys® System Configuration Guide (LIT-12011832)</td>
</tr>
<tr>
<td>Metasys UI</td>
<td>Metasys® UI Technical Bulletin (LIT-12012115)</td>
</tr>
<tr>
<td>System Configuration Tool (SCT) Software</td>
<td>Metasys® SCT Help (LIT-12011964)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This LIT number represents a print-friendly version of the Help.</td>
</tr>
<tr>
<td>Metasys System Security and Permissions</td>
<td>Security Administrator System Technical Bulletin (LIT-1201528)</td>
</tr>
<tr>
<td>Network Automation Engine (NAE)</td>
<td>NAE Commissioning Guide (LIT-1201519)</td>
</tr>
<tr>
<td>Direct Connections or Dial-up Connections</td>
<td>Metasys System Extended Architecture Direct Connection and Dial-Up Connection Application Note(LIT-1201639)</td>
</tr>
<tr>
<td>How to License the ADS/ADX</td>
<td>Software Activation Manager Help (LIT-12012389)</td>
</tr>
</tbody>
</table>
Index

M
McAfee ................................................................. 110

R
Rename ............................................................... 81
Rename a Computer ........................................... 81

S
Symantec Endpoint Protection ......................... 109

V
Virus Software ................................................... 109, 110

W
Windows Firewall .............................................. 100, 103