



AVEVA™ System Monitor

1.6

© 2015-2024 AVEVA Group Limited and its subsidiaries. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, photocopying, recording, or otherwise, without the prior written permission of AVEVA Group Limited. No liability is assumed with respect to the use of the information contained herein.

Although precaution has been taken in the preparation of this documentation, AVEVA assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of AVEVA. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement. AVEVA, the AVEVA logo and logotype, OSIssoft, the OSIssoft logo and logotype, Archestra, Avantis, Citect, DYNsIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelaTrac, InTouch, Managed PI, OASyS, OSIssoft Advanced Services, OSIssoft Cloud Services, OSIssoft Connected Services, OSIssoft EDS, PIPEPHASE, PI ACE, PI Advanced Computing Engine, PI AF SDK, PI API, PI Asset Framework, PI Audit Viewer, PI Builder, PI Cloud Connect, PI Connectors, PI Data Archive, PI DataLink, PI DataLink Server, PI Developers Club, PI Integrator for Business Analytics, PI Interfaces, PI JDBC Driver, PI Manual Logger, PI Notifications, PI ODBC Driver, PI OLEDB Enterprise, PI OLEDB Provider, PI OPC DA Server, PI OPC HDA Server, PI ProcessBook, PI SDK, PI Server, PI Square, PI System, PI System Access, PI Vision, PI Visualization Suite, PI Web API, PI WebParts, PI Web Services, PRiSM, PRO/II, PROVISION, ROMeo, RLINK, RtReports, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, WindowMaker, WindowViewer, and Wonderware are trademarks of AVEVA and/or its subsidiaries. All other brands may be trademarks of their respective owners.

U.S. GOVERNMENT RIGHTS

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the license agreement with AVEVA Group Limited or its subsidiaries and as provided in DFARS 227.7202, DFARS 252.227-7013, FAR 12-212, FAR 52.227-19, or their successors, as applicable.

AVEVA Legal Resources: <https://www.aveva.com/en/legal/>

AVEVA Third Party Software Notices and Licenses: <https://www.aveva.com/en/legal/third-party-software-license/>

Contents

Welcome to AVEVA System Monitor	5
Legal information	5
Contact information	5
Release Notes	7
System Monitor 1.6	7
New Features and Enhancements	7
Resolved Issues	7
Known Issues	9
Additional Information	10
Get Started with AVEVA System Monitor	12
System Requirements	12
Install AVEVA System Monitor	14
Configure AVEVA System Monitor	15
System Monitor Manager configuration	16
Email Server configuration	17
Security groups	19
Port list	19
License setup	20
Work with AVEVA System Monitor	21
Login to AVEVA System Monitor	21
Alert Summary and Active Alerts pane	22
Navigation pane	23
Home	23
Configuration	24
Admin Settings	24
General Settings	25
Folder Settings	27
Category Settings	28
View users and groups	29
Add an existing user account	30
Create a new local user account	31
Change password at first login	32
Edit or Delete user accounts	33
Add an existing group	34
Edit or Delete groups	35
Monitored Machines	35
Manage group	36
Manage rules	38

Move machine	40
Rules management	41
Create a rule	41
Wonderware Event Log	42
Rule condition	46
Manifest	48
Rule overview	48
Alerts, Galaxy Diagram, and Reports	49
Alerts	49
Active Alerts	49
Wonderware Alerts	50
Heartbeat Missing	52
Galaxy Diagram	52
Re-discover Galaxy	53
Reports	54
Configuring SQL Server Reporting Service	57

Welcome to AVEVA System Monitor

Welcome to AVEVA System Monitor Documentation!

AVEVA System Monitor keeps a watchful eye on the critical performance indicators associated with your AVEVA software applications and the underlying hardware to proactively maintain healthy systems for easy maintenance and reliability.

Legal information

© 2015-2024 AVEVA Group Limited or its subsidiaries. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, photocopying, recording, or otherwise, without the prior written permission of AVEVA Group Limited. No liability is assumed with respect to the use of the information contained herein.

Although precaution has been taken in the preparation of this documentation, AVEVA assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of AVEVA. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement. AVEVA, the AVEVA logo and logotype, OSIsoft, the OSIsoft logo and logotype, Archedra, Avantis, Citect, DYNsIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelaTrac, InTouch, Managed PI, OASyS, OSIsoft Advanced Services, OSIsoft Cloud Services, OSIsoft Connected Services, OSIsoft EDS, PIPEPHASE, PI ACE, PI Advanced Computing Engine, PI AF SDK, PI API, PI Asset Framework, PI Audit Viewer, PI Builder, PI Cloud Connect, PI Connectors, PI Data Archive, PI DataLink, PI DataLink Server, PI Developers Club, PI Integrator for Business Analytics, PI Interfaces, PI JDBC Driver, PI Manual Logger, PI Notifications, PI ODBC Driver, PI OLEDB Enterprise, PI OLEDB Provider, PI OPC DA Server, PI OPC HDA Server, PI ProcessBook, PI SDK, PI Server, PI Square, PI System, PI System Access, PI Vision, PI Visualization Suite, PI Web API, PI WebParts, PI Web Services, PRiSM, PRO/II, PROVISION, ROMEo, RLINK, RtReports, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, WindowMaker, WindowViewer, and Wonderware are trademarks of AVEVA and/or its subsidiaries. All other brands may be trademarks of their respective owners.

U.S. GOVERNMENT RIGHTS

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the license agreement with AVEVA Group Limited or its subsidiaries and as provided in DFARS 227.7202, DFARS 252.227-7013, FAR 12-212, FAR 52.227-19, or their successors, as applicable.

AVEVA Legal Resources: <https://www.aveva.com/en/legal/>

AVEVA Third Party Software Notices and Licenses: <https://www.aveva.com/en/legal/third-party-software-license/>

Publication date: Thursday, November 7, 2024

Publication ID: 1402878

Contact information

AVEVA Group Limited

High Cross
Madingley Road
Cambridge
CB3 0HB. UK

<https://sw.aveva.com/>

For information on how to contact sales and customer training, see <https://sw.aveva.com/contact>.

For information on how to contact technical support, see <https://sw.aveva.com/support>.

To access the AVEVA Knowledge and Support center, visit <https://softwaresupport.aveva.com>.

Release Notes

The release notes describes the new and enhanced functionality available for AVEVA System Monitor, providing an overview of the most significant changes.

Note: The product documentation is now available on the AVEVA documentation portal. To comply with the portal guidelines, the style and tone of the documentation content has been modified. Hence, the content available on the portal may differ slightly from the documentation delivered with the product release.

System Monitor 1.6

This readme document contains important information about the AVEVA System Monitor 1.6 application. Carefully review this section for issues that have been resolved in this release, and some known issues you may encounter while using AVEVA System Monitor.

New Features and Enhancements

The following new and enhanced functionality is delivered as part of AVEVA System Monitor 1.6 release.

- This version incorporates several Cybersecurity enhancements.

Resolved Issues

AVEVA System Monitor 1.6 includes corrections for the issues listed in the following table. These issues are listed by their Defect ID (IMS number), any assigned Service Request (SR) or Case Number with a brief description of the defect..

CR/Defect Number	Service Request ID/ Case Number	Description
2901078, 3492897	N/A	40-Node: [SP2023R2] During GR upgrade from WSP2017U3SP1P01 to SP2023R2 20231103.6 build, observed exceptions for adpHostSrv and LmxProxy components.
2905394	N/A	[Domain Controller] Sentinel Service does not start on system startup. Missing Domain Controller.
201646	N/A	On a fresh install, the Rule Overview page showed a Current Manifest Version value other than

		1. The Manifest version listed on the Rules grid was supposed to show the value 1 because the out-of-the-box manifest was immediately published. However, the UI showed that the manifest had already been published more than once.
201649	N/A	Machines were added to the Monitored Machines list with an inaccurate date/time value under the Discovered Date column.
202853	N/A	Users could create multiple rules with the same name.
202877	N/A	On creating a rule to monitor a file or folder with a path longer than 100 characters, the rule was partially stored in the database and was not published in the agent manifest.
202878	N/A	On undeploying a platform that was being monitored, the Runtime Provider was stopped. Upon redeploying the platform, the Runtime Provider did not resume until the Galaxy was rediscovered
202898	N/A	"I'm Alive" emails were not sent consistently until 24 hours after enabling the notification.
202906	N/A	On reports with date parameters, the data returned was not inclusive of the end-date.
608555	N/A	Distorted UI occurred when downsizing the browser window or viewing the UI in a resolution less than 1440x900.
623127	N/A	Start Menu with the option to open AVEVA System Monitor Manager is installed on non-Manager nodes.
623129	N/A	On uninstallation, System Monitor start menu options were not

		removed.
1881074	N/A	Multiple instances of the warning “Unable to add item ‘.ItemErrorCntAlarm.AlarmInhibit’ with access path” were logged in the Logger when adding an item to a DASEngine.
1436554	N/A	It took up to five minutes for the Galaxy Diagram to reflect Alert changes to the Galaxy shape in Sentinel Manager.
1655571	960134072	Resolved the alerts generated when the client could not connect to the license server or when the license server did not have an activated license.

Known Issues

This section describes known issues that remain in the release of AVEVA System Monitor 1.6 release.

CR/Defect Number/Case Number	Description	Workaround
202854	Manually specifying a proxy server in the Local Area Network (LAN) Settings configuration dialog results in inability to access the Sentinel Manager login screen.	Use an automatic configuration script (provided by your IT department) to configure a proxy server.
2630532	40-Node: [SP2023R2]: During GR upgrade from WSP2017U3SP1P01 to SP2023R2, observed EntityCommandExecution exceptions for psmsConsoleSrv component.	N/A
2885046	[SP2023R2][Case-Sensitive SQL Server] Logger errors occurred during the configuration of the configurator through silent installation.	N/A
3454387	Agent Version 1.4 does not automatically update when	The digital signature signing was updated from AVEVA Group plc to

	<p>configured with a System Monitor Server of a higher version.</p>	<p>AVEVA Group Limited. This issue is fixed in System Monitor version 1.5 and higher. The hotfix should be installed on all AVEVA remote machines to resolve the issue.</p>
--	---	---

Additional Information

AVEVA System Monitor Documentation

The AVEVA System Monitor 1.6 application includes the following documentation set:

- AVEVA System Monitor Web Help: Online Help hosted on the AVEVA Help Viewer. You can access the Help from the System Monitor Console User Interface. The web help opens in a browser window.
- AVEVA System Monitor 1.6 Readme: A single HTML file which opens in your default browser (this file).
- AVEVA System Monitor User Guide: User guide containing information on AVEVA System Monitor in Portable Document File (PDF) format.
To view PDF files, you need Adobe Reader installed on your computer. You can download the latest version of Adobe Reader from the Adobe Corporation web site:
<http://get.adobe.com/reader/>
After installing Adobe Reader, double-click on a PDF file to view the book with Adobe Reader. You can also open a PDF book with the Adobe Reader **Open** command from the **File** menu.

These documents are also available from the product installation files and the AVEVA System Monitor download page.

The AVEVA System Monitor 1.6 Readme and the AVEVA System Monitor User Guide PDF are also available in the Documentation folder available in the path **C:\ProgramData\AVEVA\Product Documentation\AVEVA System Monitor**

Web Help Display

Web Help - Browser-based User Assistance

Web help components have been delivered in this release. Web help opens in the default browser on your local computer. Help displayed in a browser allows more dynamic and searchable user assistance including standard web browser navigation.

Typically, help content is installed on your local machine as part of the documentation library, and displays in your browser without requiring an Internet connection. To open the help, use one of the following methods (depending on the editor/UI you are using):

- Press **Help** in the Login screen.

- Open web help from its installed location:
`C:\ProgramData\AVEVA\Product Documentation\AVEVA System Monitor`

Browser Permissions for Displaying Web Help

Each browser and Windows operating system combination has its own security permissions. Using Internet Explorer (version 8, 10, or 11) as an example, you may see a dialog requesting you to "Allow blocked content" each time you invoke the web help. This dialog is triggered by the presence in the help system of JavaScript components that control internal navigation and topic display elements such as pop-up or in-place-expanding display blocks that contain text and graphical images. The text and image content is itself non-active.

You can accept each occurrence of this dialog, or you can set the following option in Internet Explorer, depending on your IT security requirements: In Internet Options, click the Advanced tab, then navigate to the Security section. Enable the Allow active content to run in files on My Computer Permissions and security settings will vary depending on your specific browser.

Get Started with AVEVA System Monitor

AVEVA System Monitor is an application that monitors and manages the performance and availability of the AVEVA System Platform system including the core software, engineered software application(s), and the related hardware and network infrastructure. It detects log and reports on system performance issues/errors/trends and monitors key system attributes, and then generates alerts when those attributes exceed defined operational limits.

When an attribute is out of operational limits, the support team (internal, systems integrator, and/or AVEVA Knowledge and Support Center) is notified, and can respond proactively to prevent production interruption or downtime. The goal is to check that your solutions' performance meets and/or exceeds expectations. It is included in the common installer for AVEVA System Platform versions 2017 U3 and later.

AVEVA System Monitor is comprised of the following components:

- **System Monitor Manager:** The **System Monitor Manager** is responsible for receiving and processing all information and conditions that come in from the machines being monitored, sending out email alerts, and storing that information in the local database.

System Monitor Manager allows you to connect to a browser-based user interface to:

- Configure **AVEVA System Monitor**
 - View the machines being monitored
 - Manage rules
 - View the health status of the production system
 - Run reports
- **System Monitor Agent Install Manager:** The **System Monitor Agent Install Manager** manages the installation of the **System Monitor Agent** and supports commands sent to the Agent via the Manager. Install the **System Monitor Agent Install Manager** on every machine that will be monitored.
 - **System Monitor Agent:** The **System Monitor Agent** maintains the manifest of user-defined rules, handles monitoring of the machine to detect unhealthy conditions, and securely communicates with the **System Monitor Manager** to report those conditions.

The **System Monitor Agent** is installed by the **System Monitor Agent Install Manager** on the System Monitor Manager machine as well as every machine being monitored.

System Requirements

AVEVA System Monitor version 1.6 is an "on-premises" application, installed on a designated server-level computer. The following prerequisites are required for implementing system monitoring:

Hardware requirements

Size	Level	Cores	RAM	HDD Space
Small System (1-20 Machines)	Minimum	6	4 GB	300 GB
	Recommended	8	8 GB	400 GB
Medium System (21-50 Machines)	Minimum	8	8 GB	400 GB
	Recommended	16	16 GB	600 GB
Large System (50+ Machines)	Minimum	16	16 GB	800 GB
	Recommended	32	24 GB	1 TB

- Super VGA (1024 768) or higher-resolution video adapter and monitor
- CD-ROM or DVD drive for installation or Network connection
- Keyboard
- Mouse or compatible pointing device

Installation requires the logged in user installing System Monitor Manager software to be an administrator on the machine. Preferable to have sysadmin privileges in SQL server.

Software requirements

AVEVA System Monitor is compatible with the software prerequisites for the latest version of the System Platform.

Monitored Machines

- **Operating System:**
 - **Long Term Servicing Channel:** Windows 10 Enterprise, IoT Enterprise 2015 LTSB (1507), Windows Server 2016 LTSC Standard and Datacenter
 - **General Availability Channel:** Windows 10 21H2 Pro, Enterprise, and IoT Enterprise
- .NET Framework 4.8 (Included with installation. Installation may require a reboot.)

For more information on the supported operating system, refer to the [GCS Technology Matrix](#).

Note: Perform clear browser cache if you want to upgrade from older version to the latest version of AVEVA System Monitor.

Port List

Important! AVEVA System Monitor uses the following listed ports by default. Ensure that no other applications are using the listed ports.

- **25:** SMTP Email Notification (for non-secure SMTP)
- **465:** SMTP Email Notification (for secure SMTP)

Install AVEVA System Monitor

The FULL/Licensed mode of AVEVA System Monitor 1.6 requires an activated license. You can install the License Manager and License Server on the System Monitor Management server or configure the system to point to a remote License Server.

Notes:

- You must install AVEVA System Monitor as a Standard account user. You cannot install System Monitor if you are a Service account user, because it will not have write permission to the Program Data folder.
 - Before you reinstall System Monitor Manager on a machine, ensure that the pre-existing System Monitor Manager is uninstalled and System Monitor Database is deleted from the machine.
-

AVEVA System Monitor uses the account credentials of the logged-in user as default during installation. The default user is added to the AVEVA System Monitor Administrators security role and given full privileges to manage AVEVA System Monitor.

Use the AVEVA System Platform common installer to install AVEVA System Monitor for monitoring any AVEVA System Platform system of versions 2017 U3 or later.

- **System Monitor Manager** – You must install System Monitor Manager on a single machine in the system. For small or medium systems, it is recommended that the System Monitor Manager be installed on the same machine as the Galaxy Repository. On large systems, it is recommended that a server-class machine be dedicated to hosting the System Monitor Manager and the System Monitor database.

On selecting the System Monitor Manager, the System Monitor Agent Install Manager is also selected and installed.

If not already present, .NET Framework 4.8 is installed as a prerequisite. This install requires a reboot of the machine.

Also, if a compatible version of Microsoft SQL Server is not present on the system, Microsoft SQL Express is installed as a prerequisite.

Notes:

- Microsoft SQL Express is only recommended for small systems of 20 machines or less.
 - System Monitor SSRS reports are unavailable for System Monitor installations using Microsoft SQL Express.
 - SQL collation is not supported in the System Monitor build.
 - When you install SQL server express edition, the SQL server agent will not run and the following tasks of the AVEVA System Monitor Application will not work.
 - psms_job_sendalertsforheartbeating
 - psms_job_forcegalaxydiscovery
 - On demand job to Archive the Average time to resolve/accept alerts.
-

- On a fresh install of AVEVA System Platform 2017 U3 or later, the System Monitor Manager and System Monitor Agent Install Manager options are automatically selected when the Galaxy Repository is

selected. If you do not want to install the System Monitor Manager on the Galaxy Repository, clear the **System Monitor Manager** option in the customize installation area. However, you cannot clear the System Monitor Agent Install Manager option as it is required on every node in the system.

- On upgrade from an earlier AVEVA System Platform version to AVEVA System Platform 2017 U3 or later, you must first upgrade the existing software before you install the System Monitor Manager. Upon completion of the upgrade, run the AVEVA System Platform **Setup.exe** again. On the **Repair/Modify/Remove** screen, select **Modify**, and then select to install the System Monitor Manager.
- **System Monitor Agent Install Manager** – The System Monitor Agent Install Manager is installed as a common component on all machines on which other AVEVA System Platform software is installed, whether doing a fresh install or an upgrade. You cannot clear the **System Monitor Agent Install Manager** from the installation options as it is required on every node in the system. Additionally, the System Monitor Agent Install Manager should be installed on all other machines for which monitoring is desired.

If not already present, .NET Framework 4.8 is installed as a prerequisite. This install requires a reboot of the machine.

Note:

- During an upgrade, there may be a delay up to 30 minutes before the agents on the remote machines get updates and reflect the new build ID.
- If an install is interrupted by system reboot or power failure, the installation is corrupted, and there is no option to resume, repair, or remove the partial installation. Therefore, it is recommended that you configure a restore point before installing AVEVA System Monitor, as with the installation of other software.

- **SQL Server Reporting Services (SSRS) Reports** – In Licensed Mode, AVEVA System Monitor offers a set of SSRS reports that can be added to the system. To access the SSRS Reports, the SSRS must be running and configured with default configuration during the AVEVA System Monitor installation. This is required for the reports to be deployed to the server.

Configure AVEVA System Monitor

The AVEVA System Monitor contains two configuration items:

- **System Monitor Manager configuration:** The System Monitor Agent Install Manager specifies the name or IP address of the System Monitor Manager. This must be configured on every node on which the System Monitor Agent Install Manager is installed (every node that will be monitored). By default, the **System Monitor Manager Name** field displays the local machine name. If System Monitor Manager is not installed on the local machine, modify the value of this field to the name of the machine on which the System Monitor Manager is installed. This allows the System Monitor Agent to communicate with the System Monitor Manager.
- **Email Server configuration:** You can configure the name of the email server and accounts that will be used to send and receive alerts from the System Monitor Manager. This is configured on the System Monitor Manager node only, either in the Configurator or in the AVEVA System Monitor browser user interface. The email server sends email alerts generated by AVEVA System Monitor to notify personnel that an issue has been detected and may need to be addressed.

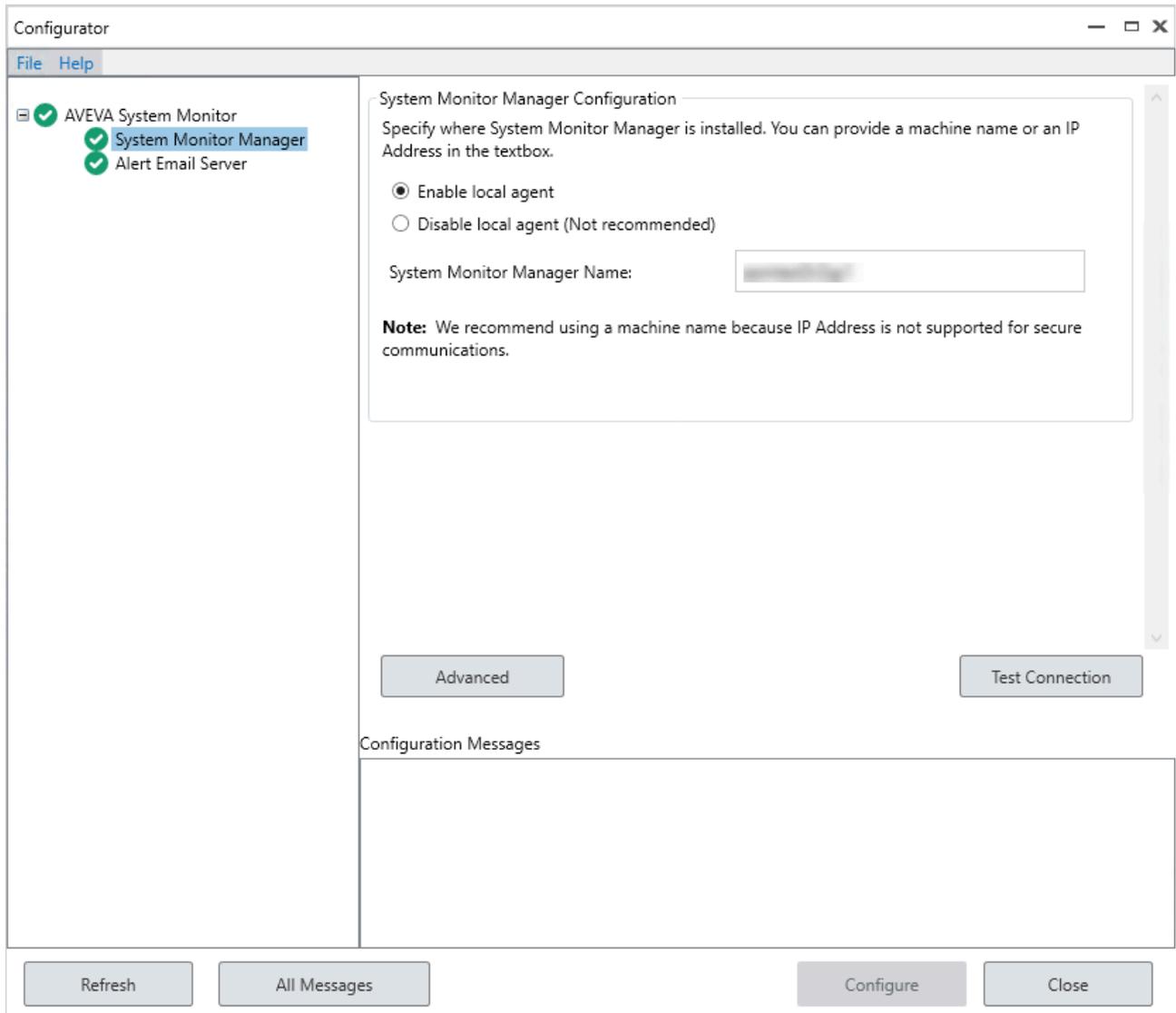
Note: You must have SQL Server administrator rights to configure the email server.

System Monitor Manager configuration

By default, the System Monitor Manager is installed on the Galaxy Repository node. There should only be one System Monitor Manager per AVEVA System Platform topology, and each node being monitored should be configured to point to it.

To configure System Monitor Manager

1. Start the **Configurator**.
2. In the left pane, under **AVEVA System Monitor**, select **System Monitor Manager**.



3. In the **System Monitor Manager Name** field, enter either the computer name (preferred) or the IP address of the node that will act as the System Monitor Manager.
If you are configuring the current node as the System Monitor Manager, enter its name or IP address. If you have configured secure communications for the Common Platform, the machine name needs to be used (the IP address is not supported for secure communications).

Note: TCP/IP is used for communications between System Monitor Agents and the System Monitor Manager.

4. Select **Test Connection** to check that the node you are configuring can reach the System Monitor Manager node.
5. Select **Configure**.
6. Select the next item in the left pane that requires configuration. When all required items have been configured, select **Close** to complete the configuration.

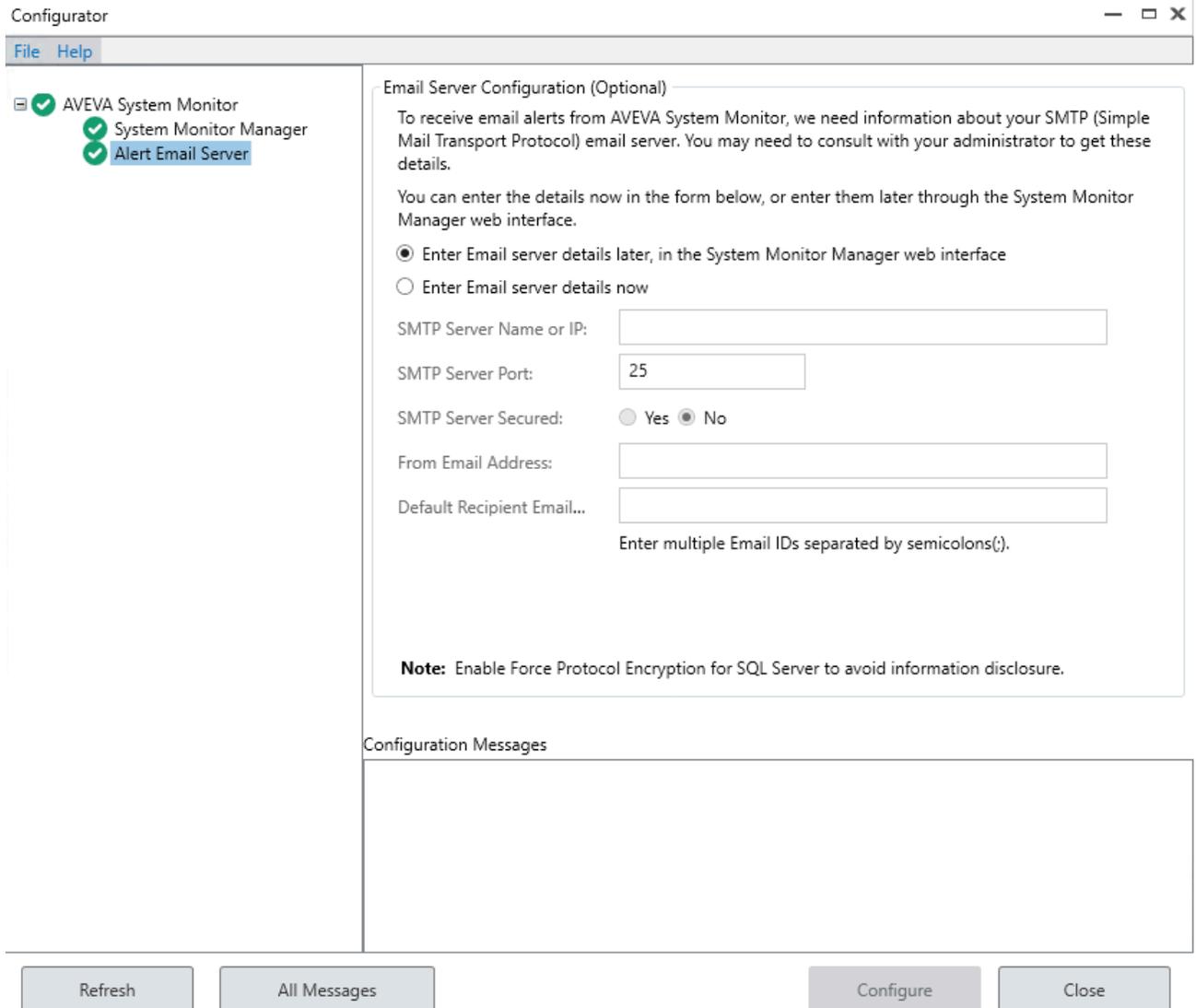
Email Server configuration

You can configure a AVEVA System Monitor Alert Email Server if you want to receive email alerts when AVEVA System Monitor identifies unhealthy conditions. The Email Server configuration is optional, and if configured, it establishes an email server that the System Monitor Manager can use to send alerts. You can configure this setting in either the Configurator or the AVEVA System Monitor browser user interface, and the two locations for configuration always stay synced.

Note: You must have SQL Server administrator rights to configure the Email Server.

To configure an email server

1. In the Configurator, under **AVEVA System Monitor**, select **Alert Email Server**.



2. Select one of the email alert details options.
 - To skip email server configuration, choose the option to **Enter Email server details later** (which can be done in the AVEVA System Monitor browser user interface).
 - To configure the email server, choose the option **Enter Email server details now**.
3. In the **SMTP Server Name or IP** field, enter either the computer name or IP address of the email server to be used for AVEVA System Monitor alerts.
4. In the **SMTP Server Port** field, enter the port number of the email server. The default is 25.
 - Use port number 25 for an unsecured SMTP server.
 - Use port number 465 for a secured SMTP server.
5. In the **SMTP Server Secured** field, select **Yes** if the server is secured, or **No** if it is not.
6. If you are using a secured email server, enter the **User Name** and **Password** to access the server.
7. In the **From Email ID** field, enter the email address that will be used to send system alerts from the AVEVA System Monitor.
8. In the **Default Recipient Email ID** field, enter the email address(es) that will receive system alerts from the

AVEVA System Monitor.

9. Select **Configure**.
10. Select the next item in the left pane that requires configuration. When all required items have been configured, select **Close** to complete the configuration.

Security groups

AVEVA System Monitor implements a group/role-based security system to control the features that are available to the logged-in user. During AVEVA System Monitor installation, the system creates the following local security groups on the System Monitor Manager:

- Administrators – full access to all AVEVA System Monitor features
- Advanced Support Engineers - Rules Management
- Support Engineers – Category/Sub-Category management, Publish Rules, Alert Management
- Configurators – Settings management
- Report Users – access AVEVA System Monitor reports
- Read-only Operators – view Active Alerts

AVEVA System Monitor User accounts are added to one or more security groups. A user who is a member of multiple security groups is granted the rights to all of the assigned groups. Typically, a user will be a member of a single group. However, the user-designated to be an Advanced Support Engineer should be a member of both the Support Engineers group and the Advanced Support Engineers group.

The AVEVA System Monitor User that is added to the AVEVA System Monitor Administrators group will be automatically added to all groups. All other users that need access to AVEVA System Monitor Reports should be added to the AVEVA System Monitor Report Users' group.

The association of the AVEVA System Monitor User account and the security group is specified using the User Management dialog in the System Monitor Manager.

Port list

The following ports are used for supporting communications between the System Monitor Manager services and the System Monitor Agent service running on the monitored computers.

- 80 [inbound] – HTTP support
- 443 [inbound] – HTTPS support (HTTP or HTTPS can be specified during installation)

The following ports are used to support SMTP email notifications:

- 25 – SMTP Email Notification (for non-secure SMTP)
- 465 – SMTP Email Notification (for secure SMTP)

License setup

AVEVA System Monitor can be installed in an unlicensed mode (BASIC Mode). In this mode, AVEVA System Monitor is limited to fully monitoring one selected machine.

AVEVA System Monitor requires a AVEVA System Monitor Activated License for full monitoring (Licensed mode) of all monitored machines. This license has an expiry date that coincides with the Customer First contract renewal date.

The un-activated XML license is installed into the License Manager and activated. AVEVA System Monitor needs to be configured to point to the associated License Server.

AVEVA System Monitor WSP 2017 U3 and later, with no activated license, will display BASIC in the **SIGN IN** dialog and will monitor the license Server(s) for all monitored machines. The **SIGN IN** dialog will display Licensed if the activated license is installed – all monitored machines will be fully monitored including the configured License Server(s).

AVEVA System Monitor, when licensed, uses activation-based licensing. Therefore, it requires an AVEVA License Server and an AVEVA License Manager from which a AVEVA System Monitor license can be acquired.

- If an activated license is detected (Licensed mode), AVEVA System Monitor provides FULL monitoring of an unlimited number of machines.
- If no activated license is detected (BASIC mode), AVEVA System Monitor provides license server and license acquisition monitoring for all machines using software that requires activation-based licensing and FULL monitoring for one machine (user-selected).

Note: The AVEVA System Monitor SSRS reports are not available in the BASIC mode.

Work with AVEVA System Monitor

This chapter describes the different functionalities of AVEVA System Monitor and how to work with them.

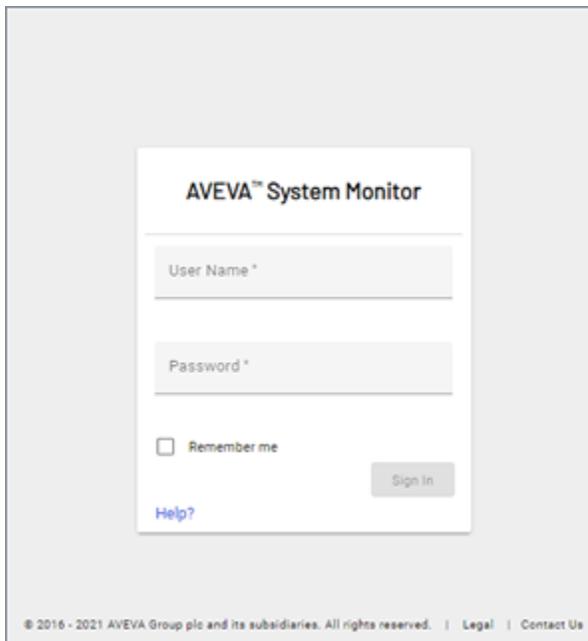
Login to AVEVA System Monitor

Note: Prior to logging into the System Monitor Manager for the first time, the URL for AVEVA System Monitor needs to be added to the Trusted Site(s) in the browser.

You can access the System Monitor Manager in two ways:

- On the System Monitor Manager machine, open the Windows Start menu, search for AVEVA System Monitor and then select the resulting browser link for System Monitor Application.
- On a machine local or remote to the System Monitor Manager, open a supported browser, and go to the following URL: *http://<nodename>/SystemMonitor*. If you are using HTTPS, go to *https://<nodename>:<port>/SystemMonitor*.

AVEVA System Monitor uses OWIN as the Internal Internet Server (IIS) to support browser-based user access. Port sharing is implemented such that both AVEVA System Monitor and IIS can share port 80. There is no requirement to disable or uninstall IIS to support AVEVA System Monitor.



The AVEVA System Monitor login page provides information about the installed version and the licensing status.

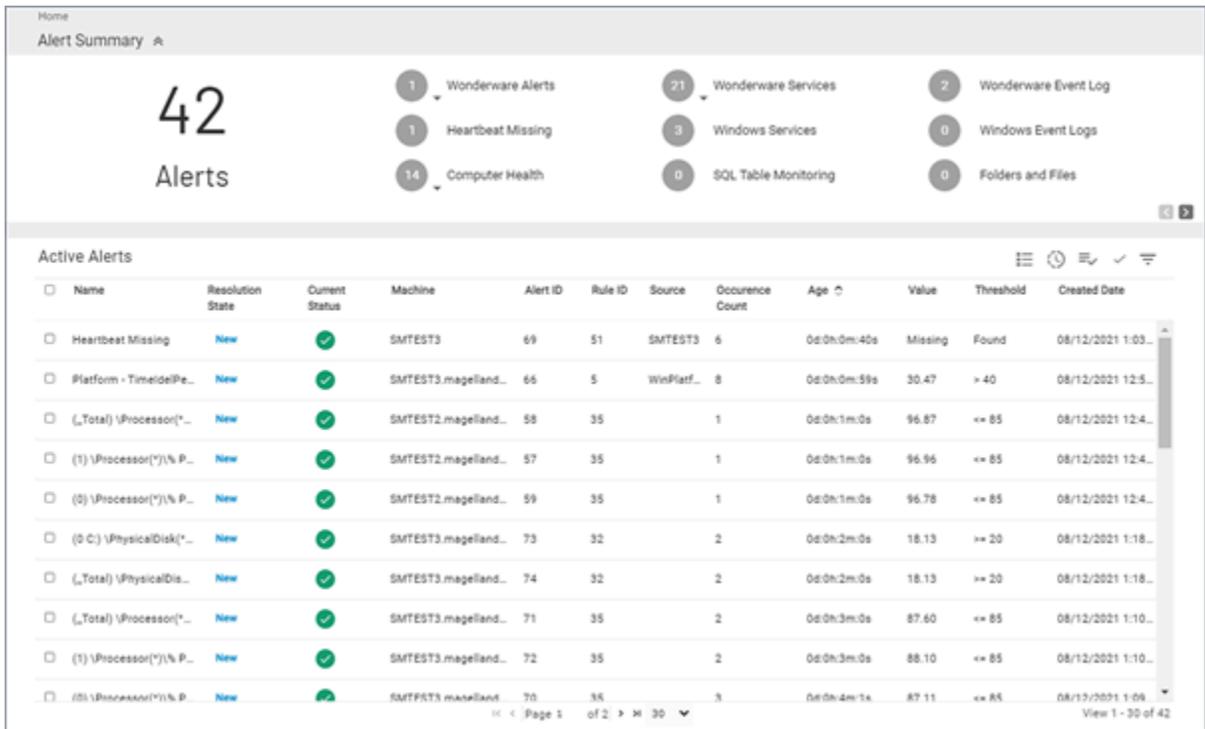
1. Select **Help** to view the AVEVA System Monitor User Guide. Note that you do not need to log in for this.
2. Provide your assigned **User Name** and **Password** and select **Sign In**.

Your credentials are validated. If the validation is unsuccessful, the system displays an error message, and the login window is displayed so that you can try again.

3. On a successful sign in, the AVEVA System Monitor **Home** screen is displayed.

The Home screen is divided into the following areas:

- the Title Bar at the top displays the current logged in user and the licensing status (right side of title bar).
- the Navigation pane on the left.
- the **Alert Summary** and **Active Alerts** pane at the center.



Alert Summary and Active Alerts pane

The **Alert Summary** pane provides summary information of the total alerts. The **Active Alert** pane provides information of the current Active Alerts totals.

The **Alert Summary** pane shows the following alerts:

- Wonderware Alerts
- Heartbeat Missing Alerts
- Computer Health Alerts
- Wonderware Service Alerts
- Window Services Alerts
- SQL Table Monitoring Alerts
- Wonderware Event Log Alerts
- Window Event Alerts
- Folders and Files Alerts

The **Alert Summary** pane is the group total indicator. Indicators to the right of the group total represent sub-group alert totals. Select a sub-group total to view the associated sub-category and alert details.

For more information, see Alerts under [Alerts, Galaxy Diagram, and Reports](#).

Navigation pane

The Navigation pane displays the major areas you use for System Monitoring:

1. [Home](#)
2. [Configuration](#)
3. [Monitored Machines](#)
4. [Rules management](#)
5. [Alerts](#)
6. [Reports](#) - The Reports area is not available when using the default SQL Server Express and requires a full AVEVA System Monitor activated license.

Each area is displayed by expanding the main (top-level) group.

Home

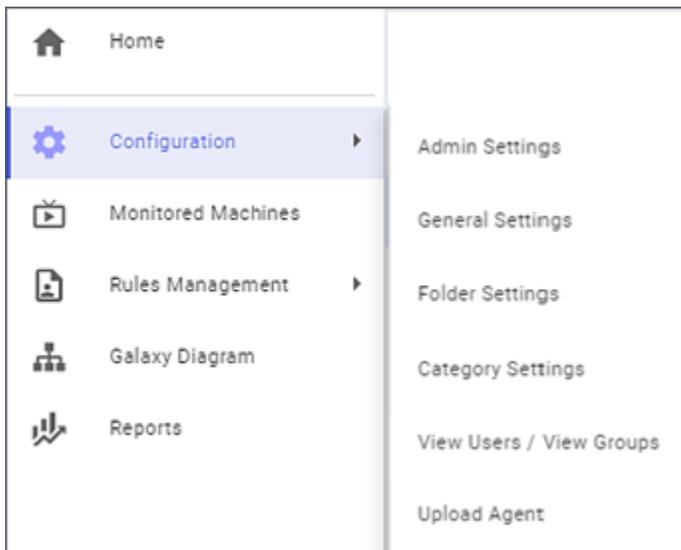
The **Home** area displays the **Alert Summary** and **Active Alerts** pane. The alerts in **Alert Summary** pane is categorized as follows:

Company Name - Alert Summary			
Total Active Alerts	Total Discovered Machines	Total Monitored Machines	
Total Wonderware Alerts (from r-h data items)	Platform Alerts	Engine Alerts	Device Integration Alerts
Total Heartbeat Missing Alerts (from r-h data items)			
Total Wonderware Services Alerts (from r-h data items)	Historian Alerts	MES Alerts	Galaxy Repository Alerts
Total Wonderware Event Log Alerts (from r-h data items)			
Total Windows Alerts (from r-h data items)	Windows Services Alerts	Windows Event Log Alerts	
Total Computer Health Alerts (from r-h data items)	Logical Disk Alerts	Network Alerts	Physical Disk Alerts

Company Name - Alert Summary			
	Processor Alerts	Per Processor Alerts	Server Alerts
	Terminal Services Alerts	SQL Server Alerts	Processor Information Alerts
Total Miscellaneous Alerts (from r-h data items)	SQL Table Monitoring Alerts	Folders and Files Alerts	

Configuration

The **Configuration** area contains the following configuration options shown below:



To know more about each option navigate to the following:

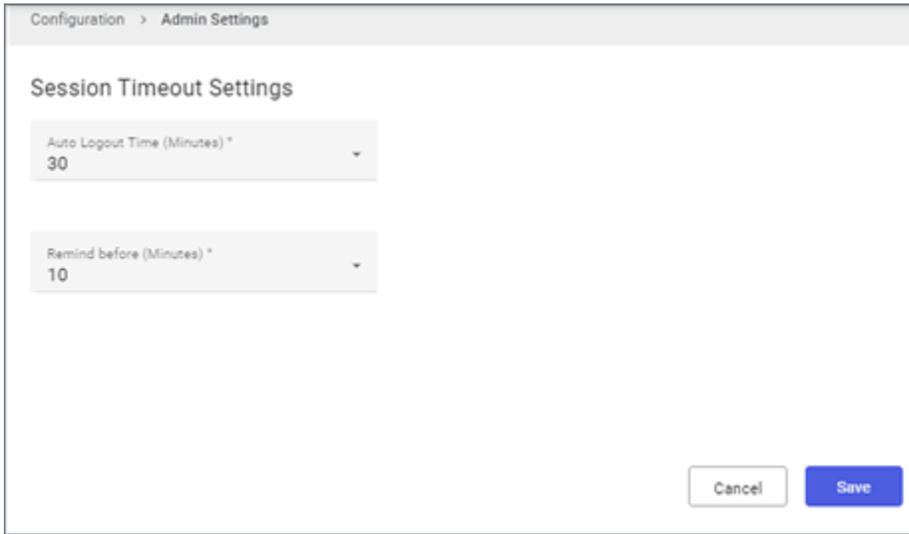
- [Admin Settings](#)
- [General Settings](#)
- [Folder Settings](#)
- [Category Settings](#)
- [View users and groups](#)

Admin Settings

The **Admin Settings** panel includes the following configuration options:

- **Auto Logout Time:** The AVEVA System Monitor session is logged out after the set time span following inactivity. Select from 30, 45, 60, 120, 240, 480, 720-minute auto log out times.
- **Remind before:** AVEVA System Monitor displays a pop-up message indicating that the system will be logged

out automatically following the reminder period if no system activity is detected. Set the Logout Reminder to be displayed 5, 10, 15, 20, 25 minutes prior to the auto log out occurring.

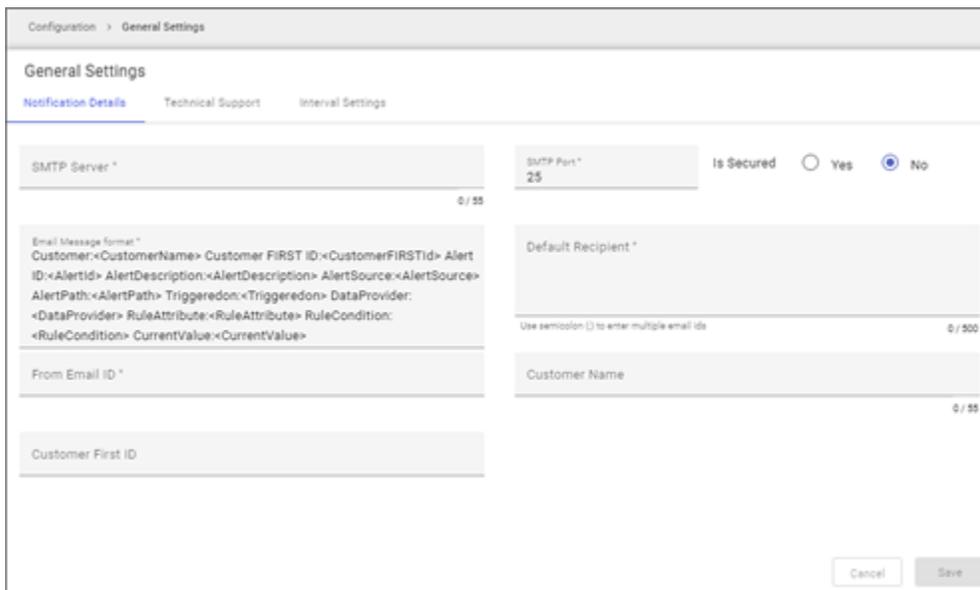


To change a setting

1. Select the drop-down list and select an interval from the list.
2. Select **Save** to save your Admin configuration changes.

General Settings

The **General Settings** panel includes **Notification Details**, **Technical Support**, and **Interval Settings**.



- **Notification Details:** In the **Notification Details** tab, enter the **SMTP Server** name and the **SMTP Port** number. Consult with your IT department for specifics regarding your SMTP email server name or IP address, SMTP port, whether the SMTP email system is secure, SMTP login credentials, and Default SMTP Recipient

(the Default Recipient entry can be a list of email addresses separated by semicolons).

- **Technical Support:** AVEVA provides remote monitoring services, you can configure AVEVA System Monitor to periodically send an email message that the notification services are working as expected. In the **Technical Support** section.

- **Enable Email I'm Alive Server-** Select **YES** to receive email messages from the AVEVA System Monitor.
- **AVEVA Software Recipient-** Add email recipient address to receive the notification status email.
- **Pinging Interval-** Select an interval to receive notification status email.
- **Interval Settings:** This area provides time interval settings for **Discovery**, **Heart Beat Period**, and **Missed Heartbeat Count**.

- The **Discovery** field defines the interval (in hours) at which Galaxy discovery is automatically performed. Discovery is executed on each monitored machine with a deployed platform, and discovers any deployment changes of engines and device integration objects that have occurred since the last discovery. This discovery is reflected in the Galaxy Diagram and the Active Alert context information.
- The **Heart Beat Period** defines (in seconds) how often each System Monitor Agent will send a heartbeat signal to the System Monitor Manager. The Heart Beat indicates the agent running as expected.
- The **Missed Heartbeat Count** specifies the number of missed heartbeats detected by the System

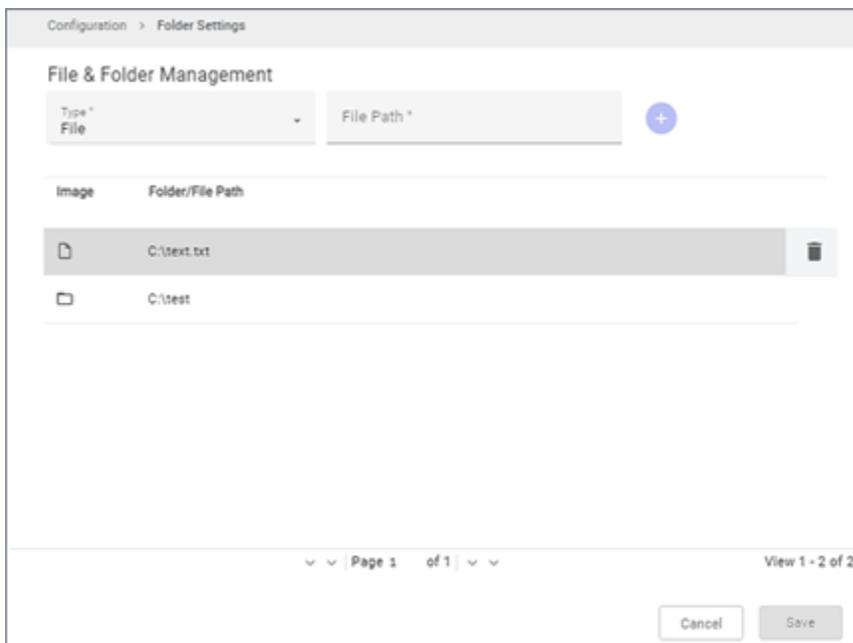
Monitor Manager (Heartbeat service) that are allowed before an Active Alert is generated for the agent machine that is not responding properly.

- The **Email Alert Frequency** applies only to License Server Alerts and controls how often an email notification is sent for a License Server Alert.
- Select **Save** to store your settings.

For information about Heartbeat Missing alert see [Heartbeat Missing](#) under Alerts.

Folder Settings

Use the **Folder Settings** to monitor specified files and folders. For example, the MES System creates work order files in a specified Work Order folder. Work orders are processed regularly, and once processed are removed or transferred to a Processed folder.



AVEVA System Monitor can execute rule(s) that monitor the count of files that exist in the designated folder and the files' creation date. If the count exceeds the accepted number of pending work orders, or the files are aging past the expected processing time, AVEVA System Monitor generates an alert and displays it in the System Monitor Manager.

To set up files and folders

1. Select the **Type** dropdown list and select **File** or **Folder**.
2. If you select **File**, provide the full path and the file name. The entry is validated, and invalid entries are indicated with a message. *A valid entry is required.*
3. If you select **Folder**, provide the full path (no trailing backslash). The entry is validated, and invalid entries are indicated with a message. *A valid entry is required.*
4. Select **Add**  to add the file to the Files and Folders grid.
5. Select **Save** to store the settings.

IMPORTANT: The file and folder names are absolute names on the machine that you expect the entries to be

found and monitored by the System Monitor Agent on that machine. Do not use a file share name or a UNC.

Category Settings

Use the **Category Settings** to edit or delete **Categories** and **Sub-Categories**.

AVEVA System Monitor monitors a broad range of health data targets, including Arcestra Runtime Attributes, AVEVA System Platform Management Console Logger, AVEVA Application Services (formerly Wonderware), Microsoft SQL Server, Computer Performance Monitor Counters and Microsoft Windows Services.

Category ID	Category	Data Provider
1	Wonderware	Runtime Data Provider
SubCategory ID	Sub Category	
3	Platform	Runtime Data Provider
4	Engine	Runtime Data Provider
7	Device Integration	Runtime Data Provider
2	Wonderware Event Log	A2Log Data Provider
4	Windows Event Logs	Windows Event log Data Provider
13	Computer Health	Perfmon Data Provider
239	Windows Services	Windows Service Data Provider

The grid displays the **Categories**. Expand the category to view the Sub-category associated with the selected category.

The Wonderware category is selected by default, and the Platform, Engine, and Device Integration sub-categories are displayed.

However, AVEVA System Monitor provides a set of common Category and Sub-Category entries out of the box, which covers the monitoring requirements of the most demanding enterprise.

To edit a Category

1. Hover on the category that you want to edit and then select **Edit Category**  .
The **Edit Category** window appears.
2. Update the **Category Name** or the **Email Notification** fields and select **Save**.

To delete a Category

1. Hover on the category that you want to delete and then select **Delete Category** .
2. Select **OK** to delete the selected Category.

Note: If the Category or sub-Categories associated with the selected category is referenced by a Rule, deletion is not allowed.

To manage Sub Categories

1. The lower grid in the Category/Sub-Category management screen displays the sub-categories associated with the Category selected in the Category grid. Manage sub-category entries by selecting a Category in the Category grid.
2. Editing and deleting a sub-category follow the same actions as described in Category management. If the **Data Provider** and/or **Email Notification** fields are specified, the entry overrides the respective setting in the parent category.

View users and groups

Selecting the **View Users / View Groups** option:

- Displays the list of domain or local users and groups assigned to AVEVA System Monitor, along with their respective roles.
- Allows you to:
 - Add an existing Domain user or Local user to AVEVA System Monitor
 - Add an existing Domain group or Local group to AVEVA System Monitor
 - Associate an existing user or group with selected AVEVA System Monitor role
 - Create a new local user account on a local machine

- Assign one or more security roles for the user or group
- Edit or Delete users or groups

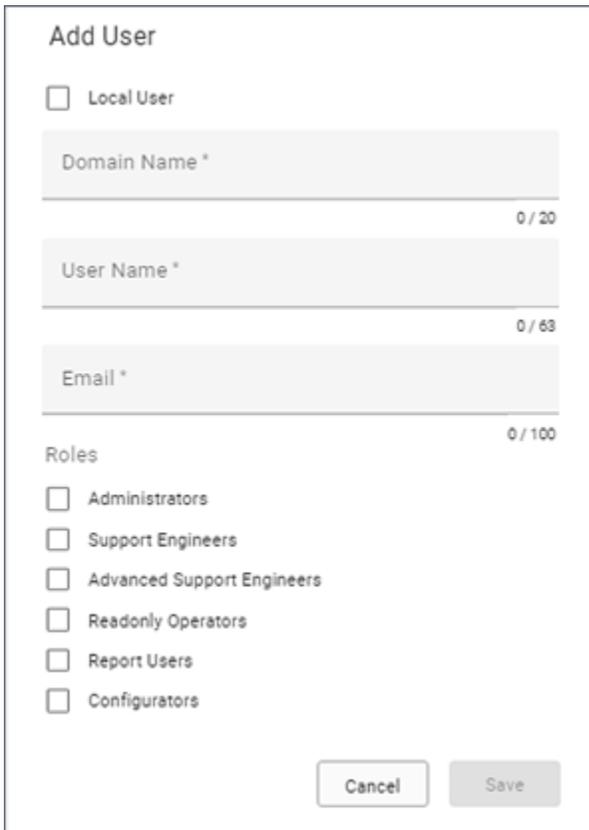
AVEVA System Monitor user account can be a domain or a local user account.

- AVEVA System Monitor Domain Users/Groups accounts are domain Users/Groups that are defined in Active Directory. The purpose of adding the user and group is to identify them with their associated roles. AVEVA System Monitor User Management sends an email to the User using the supplied email address that notifies the user of their access to the AVEVA System Monitor management system, and their permissions level. The user will then be able to sign in to the System Monitor Manager.
- AVEVA System Monitor Local User accounts are new users that are added to the local users group of the System Monitor Manager. AVEVA System Monitor automatically creates a unique password for this account. In addition, the appropriate Security groups should be selected for the user account.
- AVEVA System Monitor Local Groups are the local groups that are defined in Active Directory.

Add an existing user account

To add or assign an existing user account

1. Select **Add User**  located to the right of the **View User** grid. The **Add User** window is displayed.



Add User

Local User

Domain Name * 0 / 20

User Name * 0 / 63

Email * 0 / 100

Roles

Administrators

Support Engineers

Advanced Support Engineers

Readonly Operators

Report Users

Configurators

2. Enter the **Domain Name**, **User Name** and the **Email** address of the user.

Note: If the **Local User** check box is selected, the **Domain Name** field is hidden.

AVEVA System Monitor User Management sends an email to the user using the supplied email address that notifies the user of their access to the AVEVA System Monitor management system, and their permissions level. The user will then be able to sign in to the System Monitor Manager.

3. Select the security **Roles** that apply to this user. Security role selections are accumulative – for example, selecting **Readonly Operators** and **Report Users** grants both roles to the user.

Where applicable, the system automatically selects multiple security groups. For example, selecting **Advanced Support Engineers** automatically selects **Support Engineers**.

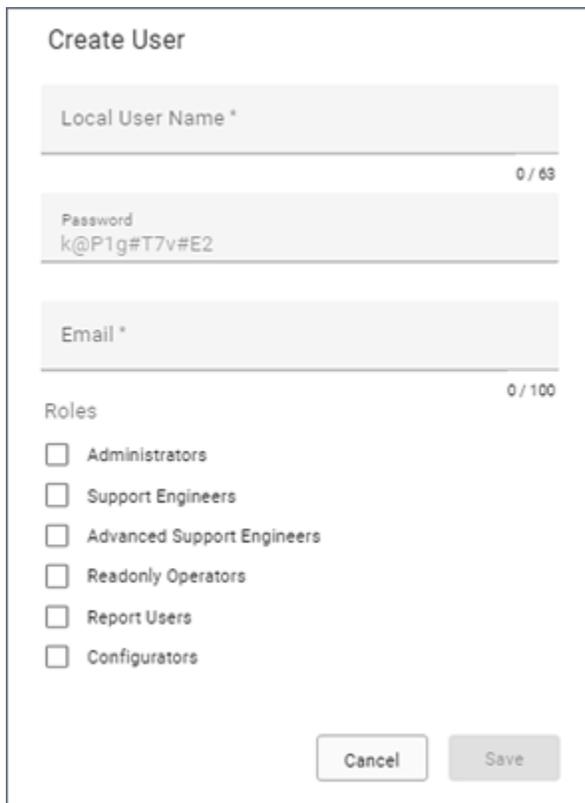
4. Select **Save** to add the user assignment to AVEVA System Monitor.

Create a new local user account

To create a new Local User account

1. Select **Create User**  located to the right of the **View User** grid.

The **Create User** window is displayed.



Create User

Local User Name * 0 / 63

Password
k@P1g#T7v#E2 0 / 63

Email * 0 / 100

Roles

- Administrators
- Support Engineers
- Advanced Support Engineers
- Readonly Operators
- Report Users
- Configurators

2. Enter the **Local User Name**, **Password**, and **Email** in the respective fields.
3. Select the security **Roles** that apply to this user
4. Select **Save**.

This action adds the user to the local machine User accounts and as members of the selected Roles (user groups). This action also stores the information and sends an email to the user at the specified email address that includes the User ID, temporary password, and permissions level. When a new user is added to the local

machine, the user is required to change their password the first time they sign in to AVEVA System Monitor.

Note: User credentials are not stored in the AVEVA System Monitor database.

The saved user information is displayed in the **View Users** tab.

User ID	User Name	Email	
5	SMTEST2\ASEUser	testase@aveva.com	Support Engineers, Advanced Support Engineers
4	SMTEST2\SupportUser	testsupport@aveva.com	Support Engineers
3	SMTEST2\AdminUser	testadmin@aveva.com	Administrators, Support Engineers, Advanced Support...

Change password at first login

To change the password

When a user signs in to the AVEVA System Monitor for the first time, the user is prompted to change their password. The **Change Password** window appears.

AVEVA™ System Monitor

Change Password

Current Password *

New Password *

0 / 18

Confirm New Password *

Skip Submit

© 2016 - 2021 AVEVA Group plc and its subsidiaries. All rights reserved. | [Legal](#) | [Contact Us](#)

1. In the **Current Password** field, enter the temporary password generated by the system.
2. In the **New Password** field, enter the new password.
3. In the **Confirm New Password** field, enter the new password again.
4. Select **Submit**.

The new password is successfully updated.

If you wish to change the password later, select **Skip**.

Note: The **Change Password** option, at the first and subsequent logins, is available only for the Local Users, and not for the Domain Users.

Edit or Delete user accounts

To edit a user account

1. Hover on the user account that you want to edit.
2. Select **Edit**  .

The **Edit** window appears. This window displays the **User Name** (not editable), **Email** address and security **Roles** (can be updated and saved for the selected user).

3. Select **Save** to save your changes.

To delete a user account

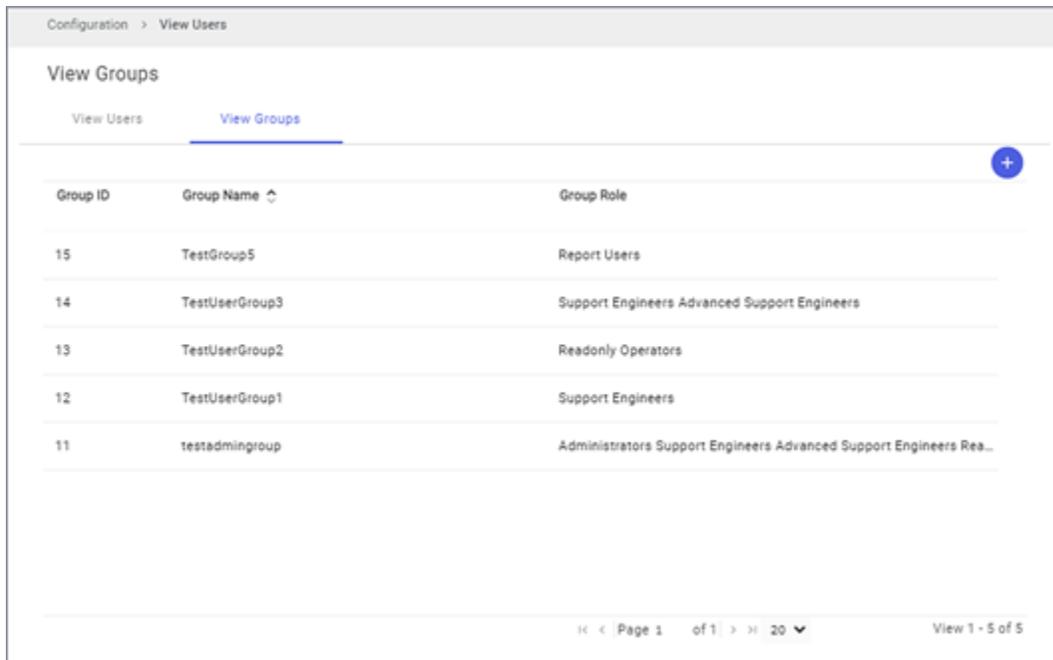
1. Hover on the user account that you want to delete.
2. Select **Delete**  .
When you delete the user, you see a confirmation message before deleting.
3. Select **OK** to delete the selected user.

Add an existing group

To add or assign an existing group

1. Select **Add Group**  located to the right of the **View Groups** grid.
The **Group Management** window is displayed.
2. Enter the **Domain Name** and **Group Name** in the respective fields.
The **Group Name** should be the same as it is mentioned in the Active Directory.

Note: If the **Local Group** check box is selected, the **Domain Name** field is hidden.
3. Select the security **Roles** that apply to this group. Security role selections are accumulative – for example, selecting **Readonly Operators** and **Report Users** grants both roles to the group.
Where applicable, the system automatically selects multiple security roles. For example, selecting **Advanced Support Engineers** automatically selects **Support Engineers**.
4. Select **Save** to add the group to AVEVA System Monitor.
Once the group is added, the users under this group will have the roles that you have assigned for that group. If a user is in two groups, then the user will have the roles of both groups.
The saved group information is displayed in the **View Groups** tab.



Group ID	Group Name	Group Role
15	TestGroup5	Report Users
14	TestUserGroup3	Support Engineers Advanced Support Engineers
13	TestUserGroup2	Readonly Operators
12	TestUserGroup1	Support Engineers
11	testadmingroup	Administrators Support Engineers Advanced Support Engineers Res...

Edit or Delete groups

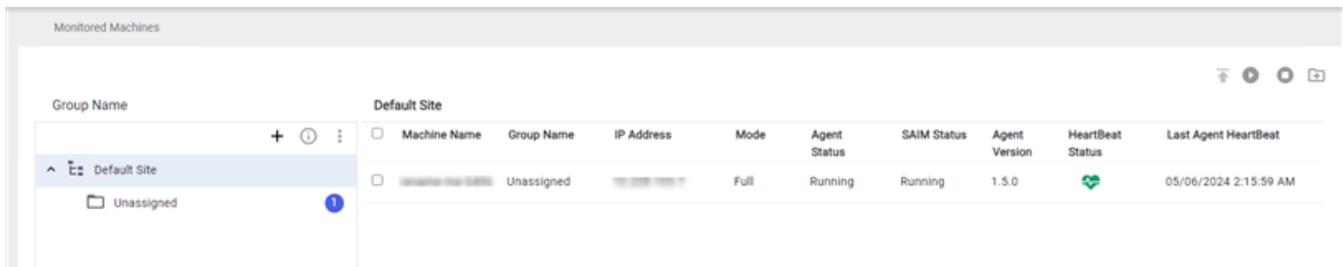
To edit or delete a group

1. Hover on the group that you want to edit or delete.
2. Do one or both of the following:
 - Selecting **Edit Group**  shows the **Edit** window. You can edit the security roles and save the changes.
 - Selecting **Delete**  deletes the selected group: When you delete the group, you see a confirmation message before deleting.

Note: This action deletes the group only from AVEVA System Monitor, not from the Active Directory.

Monitored Machines

The **Monitored Machine** list displays the machines in hierarchical order that have the System Monitor Agent installed, and which are being monitored actively.

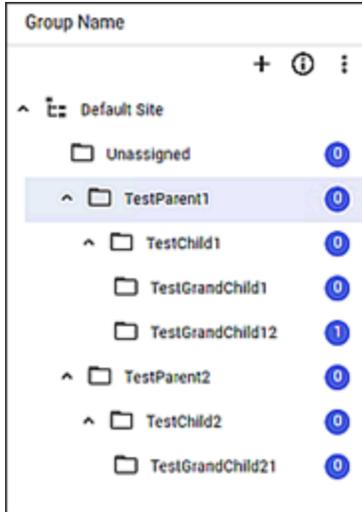


Group Name		Default Site								
Machine Name	Group Name	IP Address	Mode	Agent Status	SAIM Status	Agent Version	HeartBeat Status	Last Agent HeartBeat		
	Unassigned		Full	Running	Running	1.5.0		05/06/2024 2:15:59 AM		

The Monitored Machines area displays the following information:

- **Machine Name:** Displays the Sentinel Agent machine name.
- **Group Name:** Displays the name of the group associated with the Agent machine.
- **IP Address:** Displays the IP address of the agent machine.
- **Mode:** Indicates whether the agent node is under Full monitoring or Basic monitoring.
- **Agent Status:** Displays the Sentinel Agent service status (Running or Stopped).
- **SAIM Status:** Displays the Sentinel Install Manager service status in the agent node (Running or Stopped).
- **Agent Version:** Displays the version of the installed Sentinel Agent.
- **Heartbeat Status:** Indicates whether the Agent service is running (indicated by Green heart) or the Agent service is stopped (indicated by Red heart).
- **Last Agent Heartbeat:** Displays the Agent heartbeat, which is updated to the Manager every 10 seconds.

The Monitored Machine pane displays the groups. The groups are assigned to the **Default Site** and each group can be nested into another group. The machines are displayed in three levels of hierarchy.

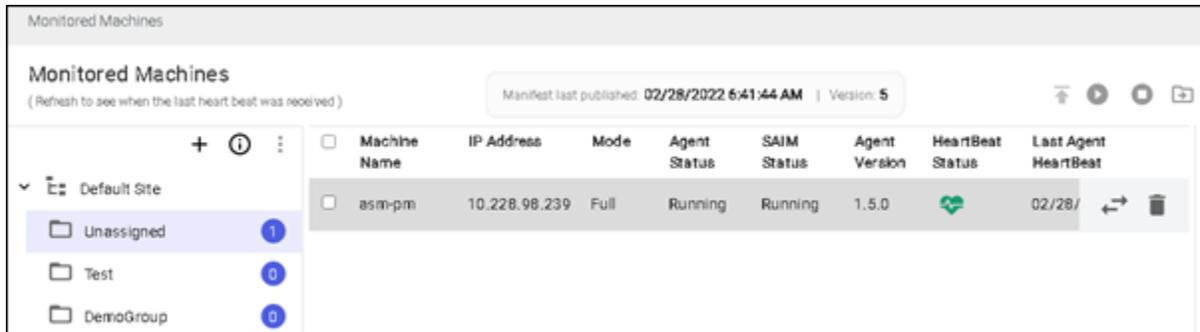


More About Mode

In unlicensed or BASIC mode, only one machine will be fully monitored. By default, the first machine to be configured will be set to FULL. You can set any machine to be fully monitored.

To set a machine to be fully monitored

1. In the **Monitored Machines** grid, select a machine by selecting the machine entry row.
2. Hover on the selected row.



3. Select  **Change to Full Monitoring Mode** icon. The selected machine is set to FULL and the previous FULL monitored machine is set to BASIC.

Manage group

To create a group

1. Select  **Add group** icon.
The **Create Group** window displays.

2. In the **Parent Group Name** field, enter the parent group in which you want to create a group.
3. In the **Group Name** field, enter the name of the group.
4. In the **Description** field, provide a brief description of the group name entered.
5. Select **Ok**.

The group is added successfully added to the Monitored Machine pane.

To modify group

1. On the Monitored Machine pane, select  **More Actions** icon.
2. Select **Modify Group**.

The **Modify Group** window appears.

3. Select the **Machine Group** name from the drop down list. By default, the parent group of the modifying machine is displayed.

Note: Select the Machine Group name which are above the level of modifying machine.

4. Update the **Group Name** and **Description** as per requirements.
5. Select **Ok**.
The group is updated with the latest changes.

To delete group

1. On the Monitored Machine pane, select  **More Actions** icon.
2. Select **Delete Group**.
3. A confirmation message appears, select **Ok** to delete the group.

To clone group

The **Clone Group** option creates a copy of a group along with the rules associated to that group.

1. Select the group you wish to clone.
2. On the Monitored Machine pane, select  **More Actions** icon.
3. Select **Clone Group**.

The **Clone Group** window appears.



4. In the **Group Name** field, enter the name of the group.
5. In the **Description** field, provide a brief description of the group name entered.
6. Select **Ok**.

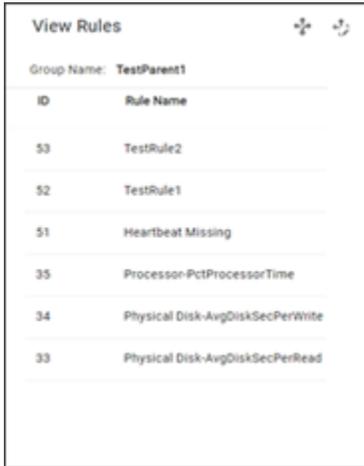
The new group is successfully cloned under the parent group, and it includes the rules.

Manage rules

To view rules

1. Select a group from the Monitored Machine pane.

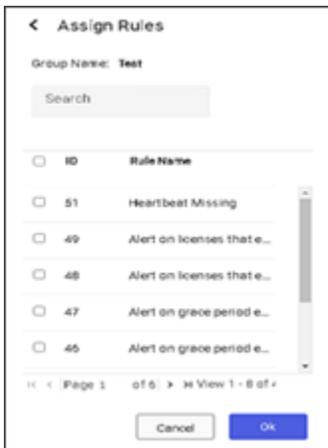
2. Select  **View Rules** icon.
The **View Rules** window is displayed.



3. The **Group Name** indicates the rules belonging to a particular group.
The rules are listed with rule **ID** and **Rule Name**.

To add rules

1. On the **View Rules** window, select  **Add Rules** icon.
The **Assign Rules** window is displayed.



2. Select the checkboxes for the rules you wish to add to the group. You can search a rule name with the help of the **Search** field.
3. Select **Ok**.
4. Select the  **Publish Manifest** icon to publish the manifest file.
The rules are successfully added to the group.

To Modify rules

1. On the **View Rules** window, select  **Modify Rules** icon.

The **Un-Assign Rules** window is displayed.



2. Select the checkboxes for the rules you wish to remove from the group.
3. Select **Ok**.
4. Select the  **Publish Manifest** icon to publish the manifest file.

The rules are successfully removed from the group.

Move machine

To Move Machine

Each machine is assigned to a group in the monitored machine pane. The machines are displayed in the Monitored Machines area with the details regarding the group name. From the list of machines displayed, you can select the machines and move them to different groups.

To move the machine to a different group

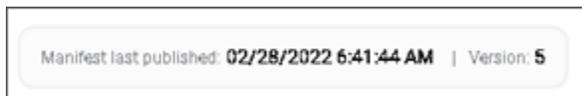
1. Select the machine you would like to move.
The **Move Machine** option is enabled.

2. Select the  **Move Machine** icon.

The **Move Group** window appears.



3. From the **Machine Group** drop-down, select the group name to which you wish to move the machine.
4. Select **Move and Publish**. The Manifest file and version number is automatically updated.
The machine is successfully moved from one group to another.



The **Manifest last published** indicates the date and time the manifest file is published. When a machine is modified, added, or moved from one group to another, the manifest file is updated. The **Version** number is incremented by one every time a new manifest file is published. The version number change is reflected on the groups that were modified.

Rules management

This chapter describes how to create and manage rules within the AVEVA System Monitor application.

Create a rule

To create a rule

1. Select **Create Rule**.
The **Rule Creation Form** is displayed.

2. In the **Rule Name** field, type a name for the rule.
3. Select a Category from the **Choose Category** dropdown list.
4. Select a Sub-Category from the **Choose Sub Category** list.
This list is updated with associated Sub-Categories for the selected Category.
5. The **Data Provider** field is set to the lowest level defined Data Provider set in the Category/Sub-Category hierarchy.
6. In the **Conditions** grid, you can add up to four conditions for each rule.

Wonderware Event Log

To add a rule condition for Wonderware Event Log

1. Select **Create Rule**.
The **Rule Creation Form** displays.

2. In the **Rule Name** field, enter a name for the rule.
3. Select **Wonderware Event Log** from the **Choose Category** dropdown list.

Note: **Choose Sub Category** dropdown list is disabled.

4. The **Data Provider** field is set to **A2Log Data Provider** which is the default data provider.
5. Select **Add Condition** in the upper-right of the **Conditions** grid.
The **Add Condition** window is displayed.
6. Select the log type from the **Select Log Type** dropdown list.
7. Add conditions for the following Log type:
 - a. **Generic:** Select **Generic** log type to trigger alerts based on the default rule.

Add Condition

Select *
Generic

Log Flag*

- Error
- Warning

Cancel

OK

Select single or multiple checkboxes from the following **Log Flag** options:

- a. **Error**
 - b. **Warning**
- b. **Component**: Select **Component** log type to trigger alerts based on the component that is generating the rule.

Add Condition

Select *
Component

Component *

Log Flag*

Error

Warning

Info

Cancel OK

Enter a value in the **Component** field.

Select single or multiple checkboxes from the following **Log Flag** options:

- a. **Error**: Alerts when errors come in from this component.
 - b. **Warning**: Alerts when warnings come in from this component.
 - c. **Info**: Alerts when info messages come in from this component.
- c. **Search String**: Select **Search String** log type to trigger alert based on a particular string. This will allow users to track for specific logger messages.

Add Condition

Select *
Search String

Search String *

Log Flag*

- Error
- Warning
- Info

Cancel OK

Enter a specific value in the **Search String** field.

Note: Use wildcards such as asterisk (*) to represent multiple characters or question marks (?) and percent (%) to represent single characters, respectively.

Select single or multiple checkboxes from the following **Log Flag** options:

- a. **Error:** Alerts when errors come in that have this string.
- b. **Warning:** Alerts when warnings come in that have this string.
- c. **Info:** Alerts when info messages come in that have this string.

Note: If you add a condition to A2Logger component, then the system displays only the **Info** checkbox for the subsequent condition.

8. Select **OK** to add the rule to the **Conditions** grid.

Note: You can configure up to four conditions for the log monitoring rule.

9. When you finish, select **Save and Publish**. The saved rule are added to the updated manifest.
You can view the log details in the Operations Control Management Control and Event Viewer

Rule condition

A rule condition defines the metric variable that you monitor, such as a Platform Object attribute, a Windows Service, or a Windows operating system Performance Counter object. You can add multiple conditions for each

rule.

To add a Rule Condition

1. Select **Add Condition**  in the upper-right of the **Conditions** grid. The **Add Condition** window is displayed.

2. Select an Attribute from the **Attribute** list.
3. The Data Type field displays the data type of the selected Attribute, and the Healthy Condition operator list is updated with valid comparison operators for the selected Attribute.
4. Select the **Healthy Condition** drop-down list to see the operator list.
5. Enter the **Healthy Condition value**.
6. **Time Deadband** controls how often an alert is sent after an unhealthy condition has occurred. You can specify the number of times an alert needs to be sent.
Enter a numerical value, the default value is displayed as 1. By default, the value range for Time Deadband 0.
The Condition changes are applicable for the following data providers:
 - Runtime Data Provider
 - Windows Service Data Provider
 - IO Data Provider
 - Perfmon Data Provider
7. Select **OK** to add the Rule to the Conditions grid. You can add up to four conditions for each rule.
8. (Optional) Provide the appropriate content in the Knowledge Base fields, such as **Symptoms**, **Resolution**, and **More information**.

9. Select **Save and Continue** to save the new Rule and reload the Rule Creation entry screen.
10. Create any additional Rules as required.
11. When you finish, select **Save and Publish**. The saved rules are added to the updated manifest and published to the System Monitor Agents.

Note: While creating a rule for the Windows or Wonderware services, instead of service executable name you can use service name directly in the attribute field.

Manifest

The manifest is a configuration file that is transferred to each monitored machine. The file contains the discovery instructions (for Historian, MES, etc.), monitoring rules, and system information that defines the actions of the System Monitor Agent.

Adding a machine to the monitored list automatically causes the System Monitor Agent to be installed on each monitored machine.

The agent service starts and the agent sends the first heartbeat to the Manager.

When the heartbeat is received by the Manager, the Agent is signaled that the current manifest is available.

The agent receives and processes the manifest and begins discovery and monitoring.

When changes are made to the configuration file:

- new monitoring rules are created.
- monitoring rules are modified.

The manifest is updated and needs to be published for transfer to the monitored machines.

Rule overview

The **Rule Overview** grid displays the active rules configured in AVEVA System Monitor.

ID	Rule Name	Category	SubCategory	Default Data Provider	Show
53	TestFile	Folders and Files	Files	ID Data Provider	<input checked="" type="checkbox"/>
52	TestFolder	Folders and Files	Folders	ID Data Provider	<input checked="" type="checkbox"/>
51	Heartbeat Missing	Heartbeat Missing	Heartbeat Missing	Heartbeat Missing	<input checked="" type="checkbox"/>
50	Alert on licenses that expire within 1 day	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>
49	Alert on licenses that expire within 7 days	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>
48	Alert on licenses that expire within 30 days	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>
47	Alert on grace period expiring within 1 day	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>
46	Alert on grace period expiring within 7 days	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>
45	Alert on grace period expiring within 14 days	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>
44	License Server Sam Service	Windows Services		Windows Service Data Provider	<input checked="" type="checkbox"/>
43	License Server Core Service	Windows Services		Windows Service Data Provider	<input checked="" type="checkbox"/>
42	License Server Agent Service	Windows Services		Windows Service Data Provider	<input checked="" type="checkbox"/>
41	LMWebService	Windows Services		Windows Service Data Provider	<input checked="" type="checkbox"/>
40	License Server in grace period	License Server Alerts		License Data Provider	<input checked="" type="checkbox"/>

Initially, you need to display All rules (Enabled and Disabled rules) in **Rule Overview** grid.

You can filter the list to view All, Enabled, or Disabled rules by selecting the filter from the Enabled/Disabled drop down list.

To enable or disable a rule

You can disable rules by selecting the **Disable** button in the right column. When you Disable/Enable a Rule, you need to publish the Manifest in order to distribute the change to the deployed agents.

To create, edit or delete a rule

- **Add:** Select **Add**  at the upper-right of the rule grid. You can add a rule using the **Rule Creation Form** in the **Create a Rule** panel. Select **Save and Publish** to finish.
- **Edit:** Select the row containing the rule you want to edit. Then select **Edit Rule**  at the upper-right of the rule grid to make your changes. Select **Submit** to finish.
- **Delete:** Select the row containing the rule you want to delete. Then select **Delete**  at the upper-right of the rule grid. Select **OK** to delete or **Cancel** to stop the deletion request.

Alerts, Galaxy Diagram, and Reports

This chapter describes how to work with Alerts, Galaxy Diagram, and Reports.

Alerts

The **Alert Summary** pane contains the following alerts:

- Wonderware Alerts
- Heartbeat Missing
- Wonderware Services
- Wonderware Event Log
- Windows Services
- Windows Event Logs
- Computer Health
- SQL Table Monitoring
- Folders and Files

Select on the alert to view the associated category and sub-category. The details of the selected alert is displayed in **Active Alerts** pane.

Active Alerts

The **Active Alerts** pane shows all detected, active alerts.

Active Alerts												
Name	Resolution State	Current Status	Machine	Alert ID	Rule ID	Source	Occurrence Count	Age	Value	Threshold	Created Date	
Heartbeat Missing	New	✓	SMTEST3	69	51	SMTEST3	6	0d:0h:0m:40s	Missing	Found	08/12/2021 1:03...	
Platform - TimeidIP...	New	✓	SMTEST3.magelland...	66	5	WinPlatf...	8	0d:0h:0m:59s	30.47	> 40	08/12/2021 12:5...	
(_Total) \Processor(*...	New	✓	SMTEST2.magelland...	58	35		1	0d:0h:1m:0s	96.87	<= 85	08/12/2021 12:4...	
(1) \Processor(*)\% P...	New	✓	SMTEST2.magelland...	57	35		1	0d:0h:1m:0s	96.96	<= 85	08/12/2021 12:4...	
(0) \Processor(*)\% P...	New	✓	SMTEST2.magelland...	59	35		1	0d:0h:1m:0s	96.78	<= 85	08/12/2021 12:4...	
(0 C:) \PhysicalDisk(*...	New	✓	SMTEST3.magelland...	73	32		2	0d:0h:2m:0s	18.13	>= 20	08/12/2021 1:18...	
(_Total) \PhysicalDis...	New	✓	SMTEST3.magelland...	74	32		2	0d:0h:2m:0s	18.13	>= 20	08/12/2021 1:18...	
(_Total) \Processor(*...	New	✓	SMTEST3.magelland...	71	35		2	0d:0h:3m:0s	87.60	<= 85	08/12/2021 1:10...	
(1) \Processor(*)\% P...	New	✓	SMTEST3.magelland...	72	35		2	0d:0h:3m:0s	88.10	<= 85	08/12/2021 1:10...	
(0) \Processor(*)\% P...	New	✓	SMTEST3.magelland...	70	35		3	0d:0h:4m:1s	87.11	<= 85	08/12/2021 1:09...	
(_Total) \PhysicalDis...	New	✗	SMTEST2.magelland...	68	52		23	0d:0h:33m:54s	5.18	+ 1	08/12/2021 12:5...	
(0 C:) \PhysicalDisk(*...	New	✗	SMTEST2.magelland...	67	52		32	0d:0h:33m:54s	0.07	+ 1	08/12/2021 12:5...	

The Active Alerts pane contains the following buttons:

- Acknowledged:** The System monitor admin acknowledges that a certain rule is broken and generates an alert from the agent node.
- Waiting On:** The alert is pending action from the relevant operator.
- Accepted:** The alert is reviewed by the operator and is actively addressing it.
- Resolved:** The issue that triggered the alert has been addressed and resolved. Consequently, the alert is no longer active and is removed from the active alerts page.
- Search Filter:** Allows the filtering of alerts based on errors (all alerts fall under errors) or warnings (a2lig warnings).

Wonderware Alerts

The **Wonderware Alerts** consists of the following Wonderware Alert Groups:

- Platform
- Engine
- Device Integration

Select a Wonderware Alert Group to display the current active alerts.

Wonderware > Platform												
Name	Resolution State	Current Status	Machine	Alert ID	Rule ID	Source	Occurrence Count	Age	Value	Threshold	Created Date	
Platform - TimeidIP...	New	✓	SMTEST2.magelland...	80	5	WinPlatf...	1	0d:0h:1m:0s	0.00	> 40	08/12/2021 1:38...	
Platform - TimeidIP...	New	✓	SMTEST5.magelland...	84	5	WinPlatf...	1	0d:0h:1m:0s	0.00	> 40	08/12/2021 1:38...	
Platform - TimeidIP...	New	✓	SMTEST3.magelland...	66	5	WinPlatf...	10	0d:0h:1m:59s	0.00	> 40	08/12/2021 12:5...	

To manage active alerts

1. Select the alert you wish to manage. Alternatively, you can view only errors or warnings using the search filter option .

Active Alerts												
<input type="checkbox"/>	Name	Resolution State	Current Status	Machine	Alert ID	Rule ID	Source	Occurrence Count	Age	Value	Threshold	Created Date
<input type="checkbox"/>	Heartbeat Missing	New		SMTEST3	69	51	SMTEST3	6	0d 0h 0m 40s	Missing	Found	06/12/2021 12:4...
<input type="checkbox"/>	(_Total) \Processor(*...)	New		SMTEST2.magelland...	58	35		1	0d 0h 1m 0s	96.87	<= 85	06/12/2021 12:4...
<input type="checkbox"/>	(1) \Processor(*)\% P...	New		SMTEST2.magelland...	57	35		1	0d 0h 1m 0s	96.96	<= 85	06/12/2021 12:4...
<input type="checkbox"/>	(8) \Processor(*)\% P...	New		SMTEST2.magelland...	59	35		1	0d 0h 1m 0s	96.78	<= 85	06/12/2021 12:4...
<input type="checkbox"/>	Platform - TimeidP...	New		SMTEST3.magelland...	66	5	WinPlatf...	9	0d 0h 1m 4s	36.81	> 40	06/12/2021 12:5...

2. To update the Resolution state, select from the following states

Note: Alerts are created with a resolution state of **New**.

- **Set Resolution State:** Select from the following states,

-  - Acknowledged
-  - Waiting On
-  - Accepted
-  - Resolved

3. Hover on an active alert row to see the **Alert Options** context menu:

- **Alert Information** : Shows the alert ID, machine name, and the source.
- **View State Changes** : Shows a history of Healthy and Unhealthy state changes for each alert.
- **Comments** : Add comments for an alert, and then select **Save**.
- **Alert Context** : Shows the context details of the active alert.

Note: Manage the remaining Alert groups using the steps described above.

View Comments History

Select an alert record in the **Resolution State** column to display the list of comments entered for the alert.

Managing Multiple Alert Records

You can select multiple alerts at one time by selecting the selection box displayed in the left column of each alert record. Select all alerts by selecting the selection box displayed in the left-hand column of the Alert title bar.

After selecting multiple records, follow the same steps to set the resolution state, or enter a comment. For selections that would be ambiguous for multiple selections, the system will display an appropriate message indicating that the selection is invalid.

Alert – Rule Details

The Alert display lists the Rule ID. For full details of the rule that is associated with a specific alert:

1. Make a note of the Rule ID.
2. Open the **Rule Overview** page, select the Rule record for the target Rule ID.
3. Select  to view all details.

The SMC Logger (Filter) rule can be edited to allow all Error and Warning log records to be displayed as alerts with email notifications. In some cases, excessive errors or warnings may be generated in the logger because of unresolved IO references, etc. The logger rule can be edited to show all error/warnings, only errors, only warning alerts, the rule can be disabled too not show any logger alerts (not recommended).

Heartbeat Missing

Heartbeat Missing tab shows all the missed Heartbeat alerts. You can view the alerts generated by the AVEVA System Monitor Manager when it is no longer receiving Heartbeat from the agent.

Based on the user's configuration for **Heart Beat Period** and **Missed Heartbeat Count**, after X missed Heartbeats, an alert is generated for the agent, indicating that the System Monitor Manager is no longer receiving health information from the agent.

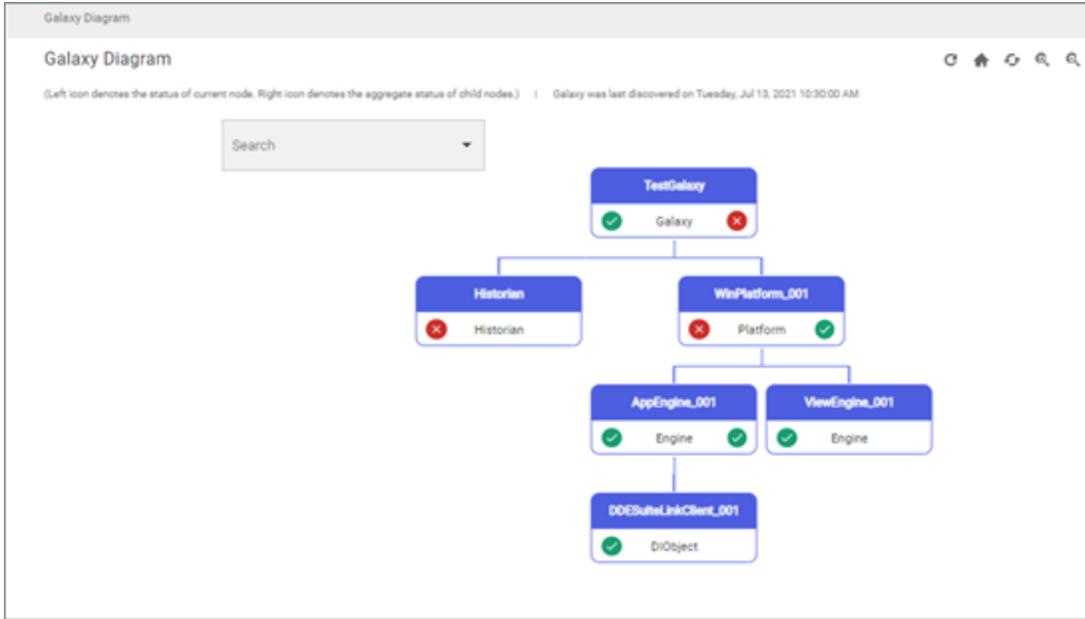
If you have configured System Monitor Alert Email Server, you will receive an email alert for Missing Heartbeat from the System Monitor Manager.

Heartbeat Missing											
Name	Resolution State	Current Status	Machine	Alert ID	Rule ID	Source	Occurrence Count	Age	Value	Threshold	Created Date
<input type="checkbox"/> Heartbeat Missing	New		SMTEST3	69	51	SMTEST3	6	0d:0h:0m:40s	Missing	Found	08/12/2021 1:03...

Galaxy Diagram

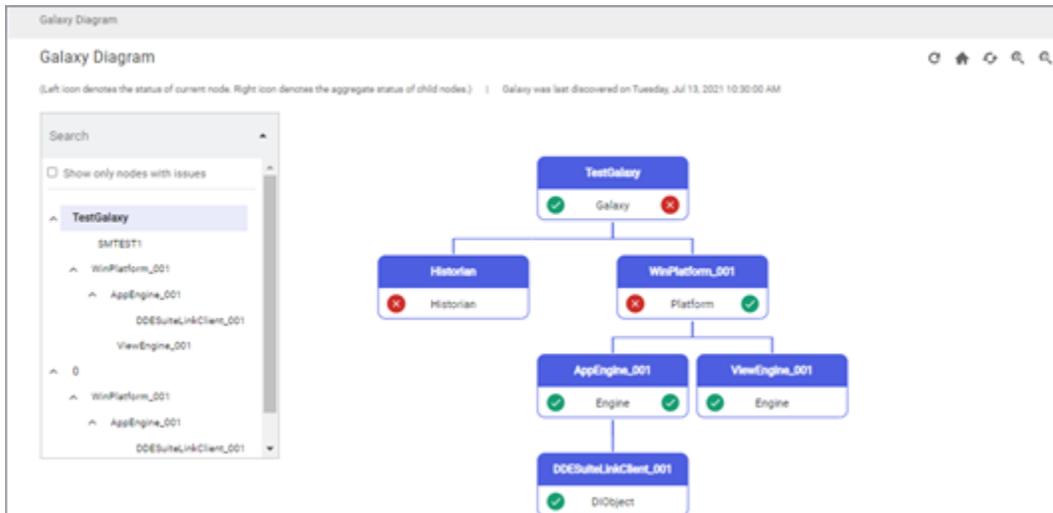
The Galaxy Diagram displays the current discovered Galaxy topology, displayed by (deployed) Platform(s), engines, and device integration objects on each monitored machine.

- Monitored items are displayed in a tree diagram as rectangles.
- The health of each item is displayed as a green check-mark icon (Healthy) or a red X icon (Not Healthy).
- The icon shown on the left side of the item indicates the health of the monitored item.
- The icon shown on the right side of the item indicates the summary health of each subordinate item.



Note: Changes to the Galaxy shape (newly deployed and/or undeployed objects, on-scan/off-scan condition, etc.) and object alert conditions can take up to 5 minutes to be refreshed and reflected in the diagram.

Select the filter box at the top of the navigation Search tree to filter all Unhealthy conditions.
Select on an object in the search tree to display the selected item and its children.



Re-discover Galaxy

The Galaxy diagram indicates the last time the Galaxy was discovered (in the upper right of the diagram).



A Galaxy includes one or more Application Servers that have:

- a deployed Platform,
- one or more engines running on each platform, and
- device integration objects running under the engine(s), if any.

The current platform, engine(s), and Device Integration objects deployed on a monitored machine constitute the current shape of the Galaxy. The shape can be easily changed within the Application Server IDE. For example, Engines and Device Integration objects can be added, deleted, transferred to another machine to run under a different Platform.

AVEVA System Monitor discovers the current shape of the Galaxy on each monitored machine on startup of the System Monitor Agent, at a specified interval as configured in the **General Settings** dialog, and can be forced to execute the **Re-discover Galaxy** option.

- Select **Re-Discover Galaxy** (the first icon in icon group in upper right of diagram) to send a command for each agent to discover the Galaxy shape. This process can take time depending on current rule processing, rule evaluation, and alert posting to the System Monitor Manager. You can select on the refresh icon to reload the Galaxy Diagram.

You can **Zoom In** or **Zoom Out** to improve the display detail of the Galaxy Diagram. The zoom options are especially useful to display a galaxy with many objects.

Select **Zoom Reset** (second icon in icon group) to redisplay the Galaxy Diagram in a 1:1 scale.

Reports

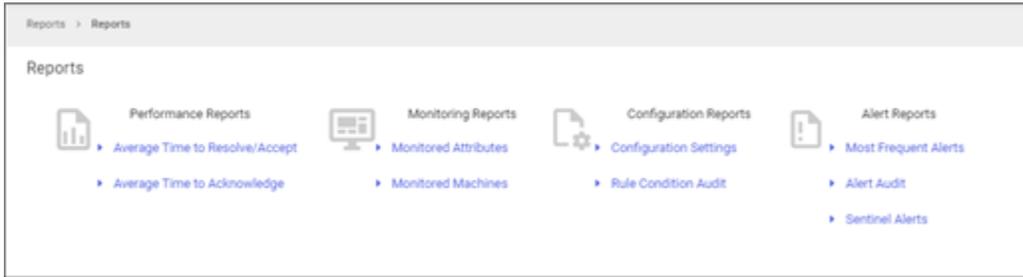
The Reports area is displayed for AVEVA System Monitor with a AVEVA System Monitor Activated License and the installation of a full SQL server or SQL Server Express that supports SSRS (SQL Server Reporting Services). SQL Server Express Enterprise and SQL Server Express Advanced support SSRS. The default SQL Server Express 2014 R2 with Tools does not support SSRS.

If you have acquired a AVEVA System Monitor license and wish to add SSRS reports to your AVEVA System Monitor installation, you must configure SSRS with the default configuration and run SSRS during AVEVA System Monitor installation. This is required for the reports to be deployed to the server.

The Reports area contains the following sub-functional topics:

- Performance Reports
- Monitoring Reports

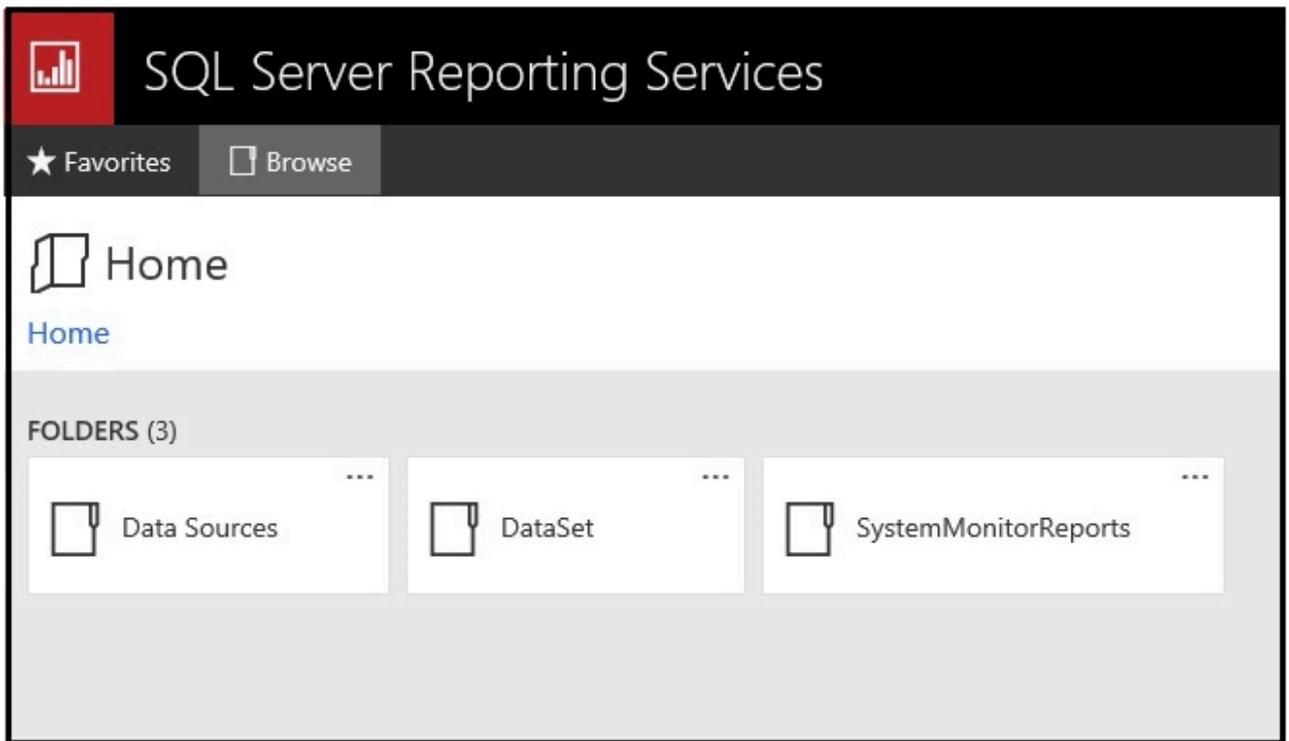
- Configuration Reports
- Alert Reports



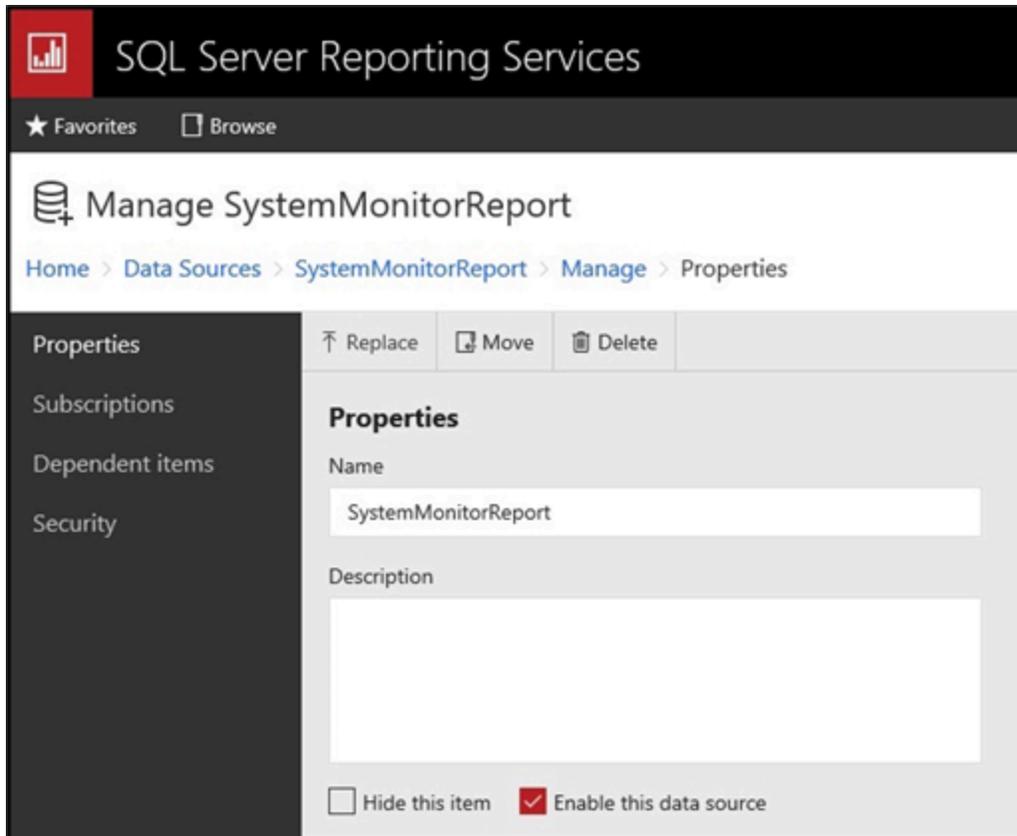
1. Select a report group to see the available reports.
2. Select a report link to generate and display the report. Some reports will request a Date Range. Supply the date range and then select **Show Report** (right side of display).

Follow the below steps to provide access to System Monitor report users

1. Go to the SQL Server Reporting Services web portal (for example: <http://<machinename>/reports>).



2. Select **Data Sources** and then select **SystemMonitorReport**.
3. In the **Properties** page, under **Credentials** section, select **Using the following credentials** and provide the user name and password which has at least data reader access to the reports server.



4. Test the connection and select **Apply**.

Credentials

Log into the data source

As the user viewing the report

Using the following credentials

Type of credentials:

Database user name and password

User name

reportuser

Password

Log in using these credentials, but then try to impersonate the user viewing the report [Learn more](#)

By prompting the user viewing the report for credentials

Without any credentials

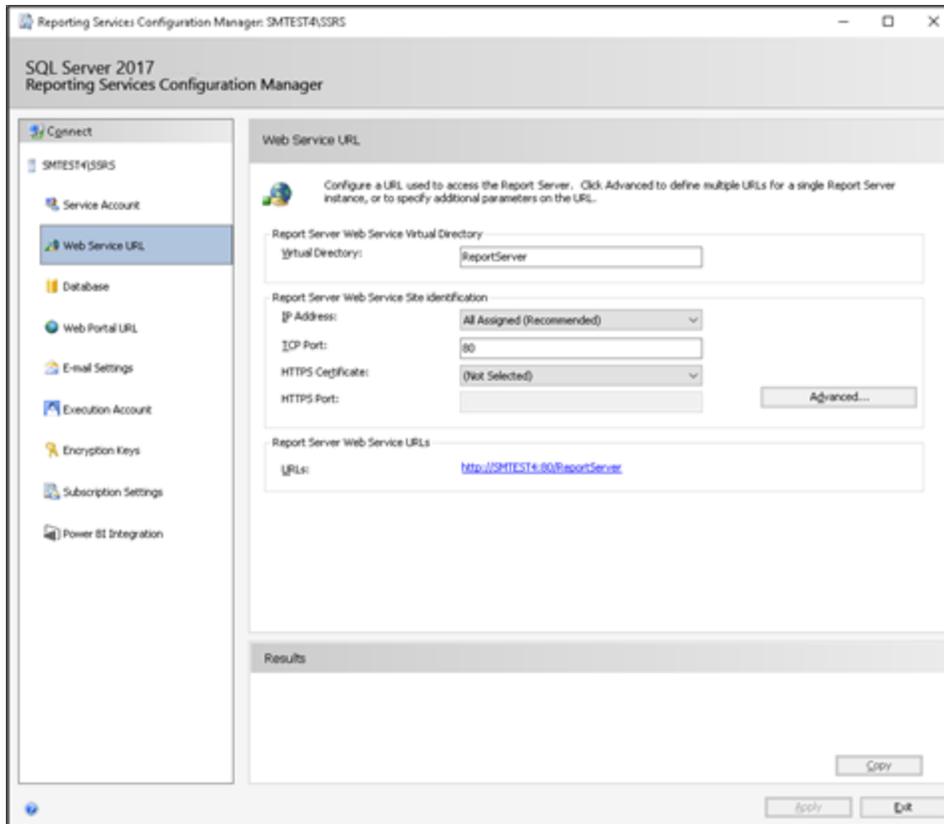
Test connection

Apply Cancel

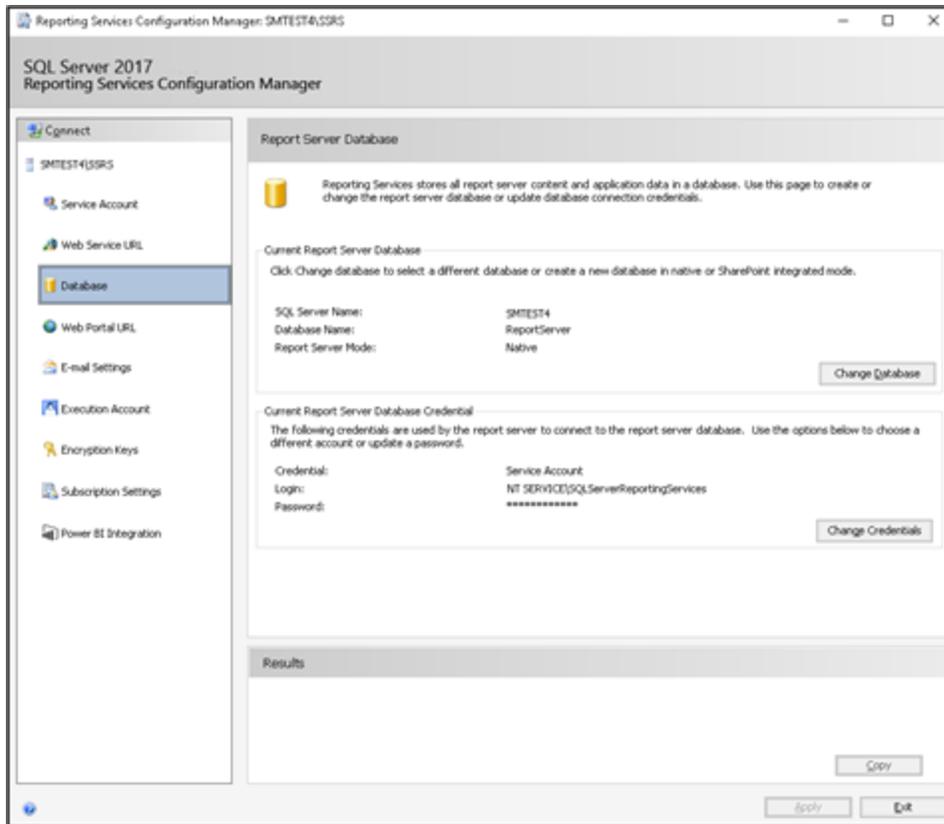
Configuring SQL Server Reporting Service

To configure SQL Server Reporting Service

1. From the **Start** menu, under **Microsoft SQL Server Reporting**, select **Report Server Configuration Manager**. The **Reporting Services Configuration Manager** window appears.
2. Configure the Web Service URL to access the Report Sever.
To configure the Web Service URL:
 - a. Select **Web Service URL** under **Connect**.
 - b. Select **Apply** with all default values.The Web Service URL is configured successfully.



3. Create the Report Server Database to store all report content and application data.
To configure the Report Service Database:
 - a. Select **Database** under **Connect**.
 - b. Select **Apply** with all default values.
 The database is created successfully.

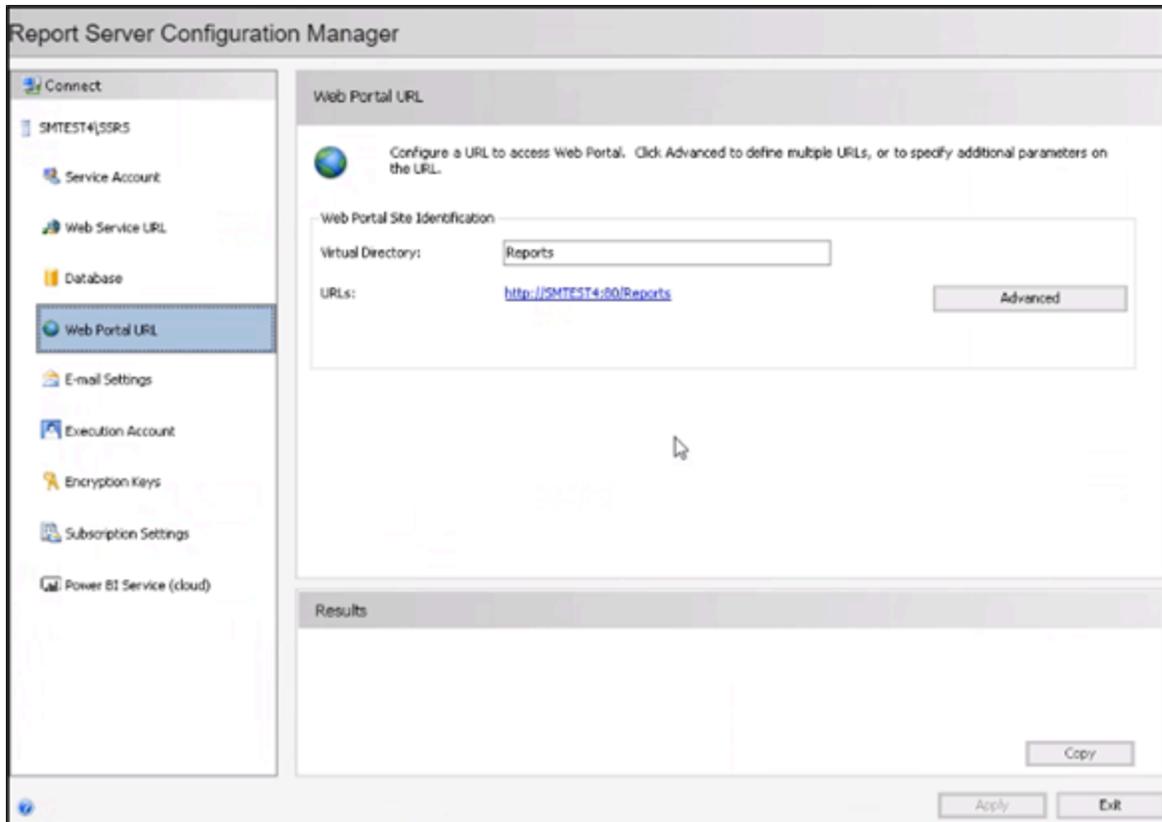


4. Create the Web Portal URL to access the Web Portal.

To create the Web Portal URL:

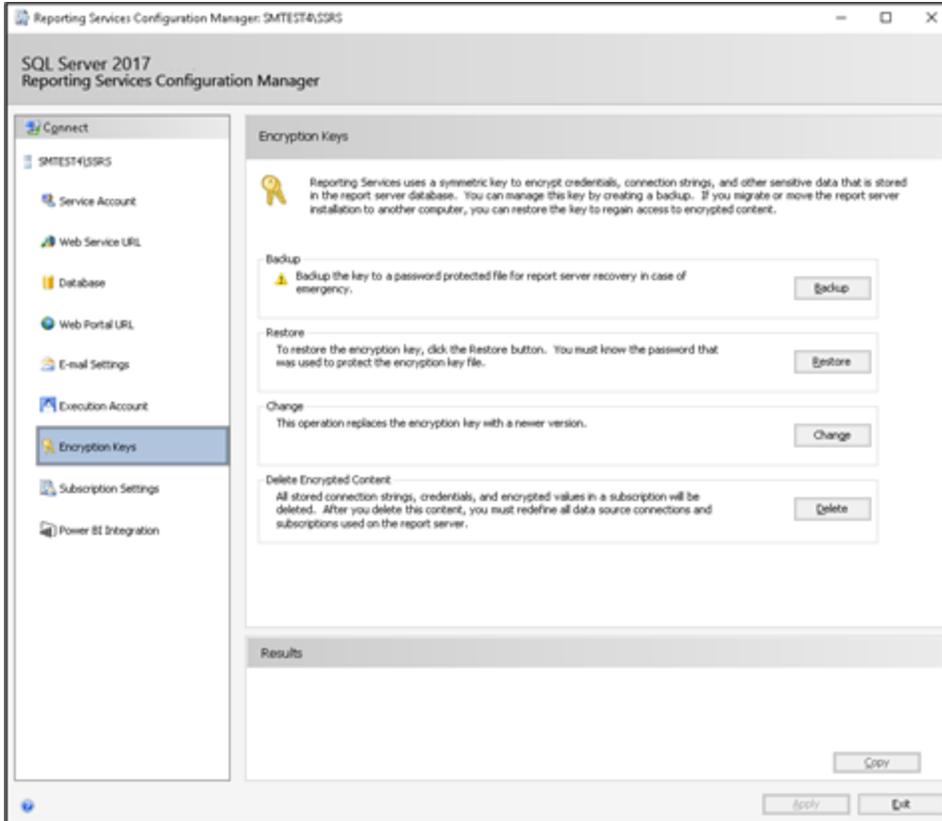
- a. Select **Web Portal URL** under **Connect**.
- b. Select **Apply** with the default values.

The Web Portal URL is created successfully.



5. To delete Encryption Keys:
 - a. Select **Encryption Keys** under **Connect**.
 - b. Under **Delete Encrypted Content**, select **Delete**.
 - c. Select **Apply**.

The encryption content is cleared successfully.



Note: The above steps are required for the installation of the SP 2020 or lower versions. For WSP 2020 R2, the reports are automatically deployed with the installation.

6. Deploy the AVEVA System Monitor reports to SQL Server Reporting Services.

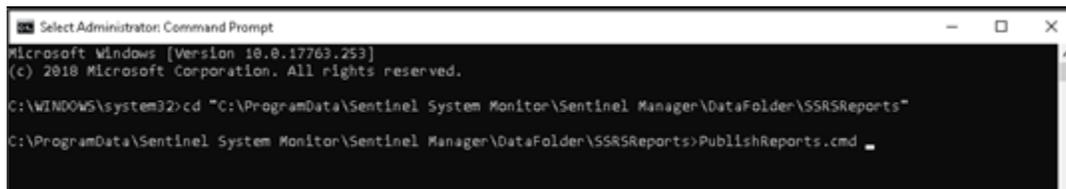
Upgrading from lower version SP 2020 / SP 2017 U3 / SP 2017 U3 SP1 to SP 2023 R2:

Case 1: If the reports are already configured and running before upgrading to WSP 2023 R2, there is no change in the SSRS installation process.

Case 2: If the reports are not configured, follow the steps below:

Note: If SSRS is installed and configured during AVEVA System Monitor installation, deploy the reports to the report server. This requires no configuration of SSRS beyond the default configuration. If the SSRS is not installed and configured during AVEVA System Monitor installation, run the **PublishReports.cmd** command by providing the parameters.

- a. After successfully installing AVEVA System Monitor, navigate to **C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports**.
- b. Open the Command Prompt as an Administrator.
- c. In the Command Prompt, navigate to the **SSRSReport** folder using the command displayed in the following screen.



- d. After successfully navigating to the folder, run the **PublishReports.cmd** command by providing the

following parameters:

Case 1: For Upgrading from lower versions to WSP 2020 R2 and higher version, and if the reports are not deployed

Parameter	Value	Comments
SQL Server Name	<SQLServerMachineName> Example: SMTEST4	Any SQL server where we are configuring the reports

The Command Prompt window appears as follows.

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd "C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports"

C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports>PublishReports.cmd http://smtest4/ReportServer SystemMonitorReports SMTEST4

C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports>SET REPORTSERVERURL=http://smtest4/ReportServer

C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports>SET REPORTFOLDER=SystemMonitorReports

C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports>SET DBSERVER=SMTEST4

C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports>rs.exe -i PublishReports.rss -s http://smtest4/ReportServer -v ReportFolder=SystemMonitorReports -v Overwrite=True -v DataSourceFolder="Data Sources" -v DataSourcePath="/Data Sources" -v filePath="C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports" -v DataSetFolder="DataSet" -v Dbname="SentinelDB" -v DbServer="SMTEST4" -v ReportName="eMgmt2018"
The command completed successfully

C:\ProgramData\Sentinel System Monitor\Sentinel Manager\DataFolder\SSRSReports>
    
```



AVEVA Group plc
High Cross
Madingley Road
Cambridge
CB3 0HB
UK

Tel +44 (0)1223 556655

www.aveva.com

To find your local AVEVA office, visit **www.aveva.com/offices**

AVEVA believes the information in this publication is correct as of its publication date. As part of continued product development, such information is subject to change without prior notice and is related to the current software release. AVEVA is not responsible for any inadvertent errors. All product names mentioned are the trademarks of their respective holders.