Server Configuration Monitor

Version 2020.2
This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
## Table of Contents

**Server Configuration Monitor Administrator Guide** .................................................. 6

**Orion Platform Documentation** .................................................................................... 7

  Orion Platform features ................................................................................................. 7

**SCM 2020.2 System Requirements** .............................................................................. 10

  Monitoring with SCM .................................................................................................. 10

  Software requirements for the Orion server ................................................................. 10

  Account privileges ..................................................................................................... 13

  Server port requirements ............................................................................................ 13

  Hardware requirements for the Orion server ............................................................. 15

  Orion database server requirements .......................................................................... 16

  Microsoft Azure deployments .................................................................................... 20

  Additional database space requirements .................................................................. 23

  SCM database monitoring requirements ................................................................... 23

  Scalability .................................................................................................................. 24

  More learning resources ............................................................................................ 24

**SCM licensing model** .................................................................................................. 25

**Node management** ..................................................................................................... 26

  Nodes supported by Server Configuration Monitor (SCM) ....................................... 26

  Add a node to SCM .................................................................................................... 26

  See nodes monitored by Server Configuration Monitor (SCM) ............................... 38

  Understand updates to asset inventory discovery in SCM ...................................... 38

  User restrictions in Server Configuration Monitor (SCM) ....................................... 38

**Monitor configuration changes on a node in SCM** .................................................... 39

  Assign configuration profiles to a node in Server Configuration Monitor (SCM) .... 39

  Unassign configuration profiles in Server Configuration Monitor (SCM) .............. 50
See detected candidates for configuration monitoring in Server Configuration Monitor (SCM) .51
Monitor Linux nodes in SCM ..........................................................52
Monitor file attributes in SCM .....................................................54
Monitor a SQL database with SCM ..............................................55
Understand database queries in SCM ...........................................60
Learn about near real-time change detection in SCM ......................60
Monitor who made server configuration changes using SCM ..........61
Enable near real-time file monitoring and 'who made the change' detection in SCM ..........64
See recent configuration changes in Server Configuration Monitor (SCM) ..................66
Enable out-of-the-box monitoring exclusions in Server Configuration Monitor (SCM) ........67
Take advantage of PowerShell script support in Server Configuration Monitor (SCM) ........69
Leverage Linux scripts in SCM ..................................................70
Test SCM profile elements before deploying them ..........................70
Change how long configuration data is kept in Server Configuration Monitor (SCM) ........74
Watch for specific configuration changes in SCM ..............................75
View the structural diff in SCM ................................................80

Server configuration profiles in SCM ........................................81

SCM out-of-the-box profiles .....................................................81
Custom profiles in SCM ..........................................................98
Import and export profiles in SCM ..............................................101
Automate SCM profile import or export ......................................102

Compare configurations over time in Server Configuration Monitor (SCM) ..................111

See configuration changes between two points in time using SCM ........111
Learn about baselines in SCM ..................................................115
Correlate configuration changes to performance metrics in SCM ........116

Azure SQL database support in SCM ........................................119

Alert on SCM data ..................................................................119
Events in Server Configuration Monitor (SCM) .................................................................120
Report on Server Configuration Monitor (SCM) data ..............................................................121
Explanations of error messages in SCM ..................................................................................123
  Server configuration errors ..................................................................................................123
  Errors assigning elements to incompatible platforms .........................................................124
  Element errors ...................................................................................................................125
Troubleshoot your SCM deployment ......................................................................................127
Troubleshoot FIM driver issues in SCM ................................................................................128
Welcome to the Server Configuration Monitor (SCM) Administrator Guide.

This guide provides an overview of product features and related technologies. In addition, it contains recommendations on best practices, instructions for getting started with advanced features, and troubleshooting information for common situations.

Here are some additional resources:

- For information about planning, installing, and getting started with SCM, see the [SCM Getting Started Guide](#).
- To install SCM, review [SCM 2020.2 system requirements](#) and [SCM 2020.2 release notes](#), and then use the [SolarWinds Orion Installer](#).
- To get the latest version of SCM, use the [SCM Upgrade Guide](#).
- Visit the SolarWinds Success Center for SCM and other SolarWinds product guides, training resources, and technical support articles.
- Check out the [Server Configuration Monitor product forum](#) in the SolarWinds online IT community, [THWACK](#), to connect with SolarWinds developers and product managers, as well as other SCM users. Download files to customize deployment and extend our product, and find out what SolarWinds is working on for SCM. Some content in this area is created by SolarWinds staff, and the rest is created and shared with the community by our members.
- For details about features shared by SCM and other Orion Platform products, see the next section in this guide—Orion Platform documentation.
Orion Platform Documentation

The following is information on the Orion Platform and Orion Web Console that is not specific to SCM, but is referenced throughout the SCM Administrator Guide. For a comprehensive look at the platform, see the online Orion Platform Administrator Guide.

Orion Platform features

The Orion Platform is the core of the SolarWinds IT Management Portfolio. It provides a stable and scalable architecture that includes data collection, processing, storage, and presentation. The Orion Platform provides common features, such as user accounts and groups, views, dashboards, reporting, alerting, and more that you can use across all Orion Platform products and access from the Orion Web Console.

Pre-installation hints

Before you install your Orion Platform products, review the following details:

Orion Platform requirements

- Hardware, software, and port requirements for the Orion Platform server and SolarWinds Orion database.

Licensing

- Licensing differs among Orion Platform products. Activate, add, upgrade, or assign licenses with the License Manager in the Orion Web Console.

Installation or upgrade

- Use the SolarWinds Orion Installer to easily install or upgrade multiple Orion Platform products simultaneously.

While installing your Orion Platform products, you might need to enable FIPS or review directories to be excluded from antivirus protection.

Common features in Orion Platform products

Learn Orion Platform basics

- Log in to your Orion Platform product in a web browser and meet the Orion Web Console.

Review events to know what’s going on.
Get alerts about issues in your environment.

Generate reports to present the status of the monitored environment.

Review Performance Analysis dashboards, also known as PerfStack™.

Create, edit, and maintain Orion Web Console user accounts - set user rights, reset passwords, limit access to network segments, and enable authentication with Active Directory.

View monitored objects on maps in the Orion Web Console - view automatically generated Orion Maps as a subview, display objects with their locations specified in the OpenStreet format in a widget, or create maps using the Network Atlas tool and display them in the Orion Web Console.

Add devices for monitoring and manage monitored devices

Specify which devices to monitor and the information you need, then select the way you get this information. See Discover and add devices.

Add single nodes, use Active Directory domain controllers to add nodes, or discover devices on your network automatically.

Available polling methods include ICMP, WMI, SNMP, and agents deployed on Windows, Linux, and UNIX devices.

Manage monitored devices - edit properties, set the polling methods for monitored devices, toggle monitoring on and off, or mute alerts for nodes.

Customize your Orion Web Console

Customize Orion Web Console - customize dashboards, colors, logos, views, widgets, and charts. Learn how to limit which objects users see on views, or specify what you want to see on views for specific devices types. Add a Performance Analysis Project to the menu.

Create custom properties - Create custom properties - create custom fields to associate with monitored network objects and display custom information for monitored devices.

Create groups and dependencies - organize how monitored data is presented in the Orion Web Console. Set up dependencies to better represent the relationships between network objects and account for constraints on the network.

Set thresholds - specify thresholds for monitored metrics. Customize general thresholds or use baselines.

Restrict user access to network areas by applying limitations, specify patterns for limitations in the Orion Platform, and create limitations based on custom properties.

Expand Orion Platform functionality or scale your deployment

Use SolarWinds High Availability (HA) to provide failover protection for your Orion server and additional polling engines to reduce data loss.
Do you need to scale your deployment? See "Scalability Engine Guidelines."

Review tips for optimizing your deployment.

Balance the load on polling engines by specifying nodes to be polled by individual polling engines.

Manage Additional Polling Engines.

Troubleshoot environmental issues with Performance Analysis dashboards or troubleshoot your SolarWinds Orion database.
SCM 2020.2 System Requirements

Release date: June 4, 2020

Important: These recommended system requirements are for SolarWinds Server Configuration Monitor (SCM) 2020.2 as a single product installed on Orion Platform 2020.2. Requirements may increase for medium or large environments, or environments with multiple modules installed.

- Monitoring with SCM
- Software requirements for the Orion server
- Account privileges
- Server port requirements
- Hardware requirements for the Orion server
- Orion database server requirements
- Additional database space requirements
- Microsoft Azure deployments
- Scalability
- More learning resources

For additional information on requirements and configurations, see the multi-module system guidelines. You should also review your product administration guides and release notes for the exact product requirements beyond these minimums. SolarWinds also recommends reviewing the SCM 2020.2 release notes.

Monitoring with SCM

- SCM 2020.2 supports monitoring on nodes running Windows Server 2008 R2 SP1 and newer and Linux kernel 2.6.23 or newer.
- SCM requires read permission to the monitored path for all file, parsed file, and registry profile elements. It requires execute permission for scripts.

SCM uses the SHA1 algorithm to compute a hash code while detecting whether a configuration item has changed on Windows and Linux machines. Although SHA1 is not an approved algorithm in FIPS mode, it is not used as a security function in SCM. Therefore, its use in SCM does not violate Federal Information Processing Standard (FIPS) 140-2 or the Cryptographic Module Validation Program (CMVP).

Software requirements for the Orion server
This table lists software requirements and recommendations for a SolarWinds installation on both physical and virtual computers.

<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>• Microsoft Windows Server 2012 R2*</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 2016</td>
</tr>
</tbody>
</table>

*Support for Microsoft Windows Server 2012 R2* is included in SCM 2020.2 so SCM 1.0 customers can upgrade to the latest version of SCM. For the best experience, SolarWinds recommends using Windows Server 2016 or 2019 for the Orion server.

**Desktop operating systems**, such as Windows 10, 64-bit (not Standard Edition), are supported for **evaluation environments only**. To make a smooth transition from your evaluation to production deployment, SolarWinds recommends that you avoid installing evaluations on desktop operating systems.

**Support differences between Orion Agents and Orion Platform products**

- You cannot install Orion Platform products on domain controllers. **Exception:** You can install Orion Agents on domain controllers.

- You cannot install Orion Platform products or any scalability engines on Microsoft SharePoint, Microsoft Exchange, or BlackBerry servers. **Exception:** You can install Orion Agents on the same server as a Microsoft SharePoint, Microsoft Exchange, or BlackBerry server.

<table>
<thead>
<tr>
<th>Operating system languages</th>
<th>English (UK or US)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>German</td>
</tr>
<tr>
<td></td>
<td>Japanese</td>
</tr>
<tr>
<td></td>
<td>Simplified Chinese</td>
</tr>
</tbody>
</table>

**IP address version**

- IPv4
- IPv6
- Dual stack

**i** CIDR notation is not supported for IPv6 addresses.
<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server</td>
<td>If you are not using Windows Authentication, make sure Anonymous Authentication is enabled for the default SolarWinds Orion website, NetPerfMon. Anonymous Authentication is used with the default, forms-based authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>i</strong> IIS is installed by the SolarWinds Orion Installer. You can install this software manually to reduce installation time or network bandwidth.</td>
</tr>
<tr>
<td>Installing Windows Account</td>
<td>Requires administrator permission on the target server.</td>
</tr>
<tr>
<td>File System Access Permissions</td>
<td>Ensure the NetworkService account has access to the system temp directory: %systemroot%\temp.</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>Version 10.0 or later. DNS specifications require hostnames to be composed of alphanumeric characters (A-Z, 0-9), the minus sign (-), and periods (.). Underscore characters (_) are not allowed.</td>
</tr>
<tr>
<td></td>
<td><strong>i</strong> SolarWinds does not support installing SolarWinds SCM on the same server or using the same database server as a Blackberry server.</td>
</tr>
<tr>
<td>Microsoft ASP .NET 2.0 Ajax Extension</td>
<td>Version 1 or later</td>
</tr>
<tr>
<td></td>
<td>If this is not found on the target computer, the Orion Installer downloads and installs the component.</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>Version 4.8</td>
</tr>
<tr>
<td></td>
<td><strong>i</strong> Run the same version of .NET on your primary server and any Additional Polling Engines (APEs) or Additional Web Servers (AWS) in the environment.</td>
</tr>
<tr>
<td></td>
<td><strong>!</strong> SolarWinds recommends installing .NET on your primary Orion server and all scalability engines before installing SCM. See this article for details.</td>
</tr>
</tbody>
</table>
### Type and Requirements

<table>
<thead>
<tr>
<th>Orion Web Console browser</th>
<th>Orion Platform products support the two most recent versions of the following web browsers available at the release date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Firefox</td>
</tr>
<tr>
<td></td>
<td>• Chrome</td>
</tr>
<tr>
<td></td>
<td>The following browsers are also supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer</td>
</tr>
</tbody>
</table>

⚠️ **Account privileges**

SolarWinds recommends that SolarWinds Orion administrators have local administrator privileges on the Orion server to ensure full functionality of local SolarWinds tools. Orion user accounts limited to the Orion Web Console do not require local administrator privileges.

⚠️ **Server port requirements**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>SSH</td>
<td>SolarWinds Job Engine v2</td>
<td>Bidirectional</td>
<td>Access ASA devices through CLI</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>Default port for SMTP email notifications. If SSL/TLS encryption is enabled on the SMTP server, use port 465.</td>
</tr>
<tr>
<td>53</td>
<td>UDP</td>
<td>SolarWinds Job Engine V2</td>
<td>Bidirectional</td>
<td>Resolving DNS queries</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>IIS</td>
<td>Inbound</td>
<td>HTTP default for the Orion Web Console</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SolarWinds Job Engine V2</td>
<td>Outbound</td>
<td>SNMP statistics collection, the default for polling</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>IIS</td>
<td>Inbound</td>
<td>Default port for HTTPS binding</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>File and Printer Sharing (SMB-In)</td>
<td>Bidirectional</td>
<td>Used to store firmware updates and configuration files remotely</td>
</tr>
<tr>
<td>465</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>Default port for SSL-enabled email alert actions</td>
</tr>
<tr>
<td>587</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>Default port for TLS-enabled email alert actions</td>
</tr>
</tbody>
</table>
| 1434 | UDP      | SolarWinds Alerting Service V2  
          SolarWinds Administration Service  
          SolarWinds Information Service  
          SolarWinds Information Service V3  
          SolarWinds Orion Module Engine  
          SQL Server Browse Service | Outbound | Communication with the SQL Server Browser Service to determine how to communicate with certain non-standard SQL Server installations. Required only if your SQL server is configured to use dynamic ports. |
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/ Process</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1801</td>
<td>TCP</td>
<td>MSMQ</td>
<td>Bidirectional</td>
<td>MSMQ WCF binding (For more information, see <a href="#">this article from Microsoft</a>)</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Bidirectional</td>
<td>For RabbitMQ messaging (AMQP/TLS) between the main polling engine and all Additional Polling Engines, High Availability servers, or Additional Web Servers.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Orion Module Engine&lt;br&gt;SolarWinds Information Service&lt;br&gt;SolarWinds Information Service V3</td>
<td>Bidirectional</td>
<td>Orion module traffic. The port used for communication between the Orion Web Console and the poller.</td>
</tr>
<tr>
<td>17778</td>
<td>HTTPS</td>
<td>SolarWinds Agent</td>
<td>Inbound to the Orion server</td>
<td>Required for access to the SWIS API and agent communication</td>
</tr>
</tbody>
</table>

*Ports 4369, 5672, and 25672 are opened by default. These ports can be blocked by the firewall.*

## Hardware requirements for the Orion server

The following table lists minimum hardware requirements and recommendations for your Orion server on physical computers, virtual computers, and cloud instances. Use the minimum hardware configuration if you are evaluating the product or do not anticipate heavy usage.

- Do not install Orion Platform products on the same server as SolarWinds Access Rights Manager (ARM).
- SolarWinds strongly suggests using the recommended hardware configuration to avoid potential performance issues caused by a heavy load or custom configurations such as increased data retention or more frequent polling intervals.
- Installing multiple Orion Platform products on the same computer may change the requirements.
## Orion database server requirements

The following table lists software and hardware requirements for your SolarWinds Orion database server using SCM license levels. You **must** create the SolarWinds Orion database with the SolarWinds Configuration Wizard. Creating the database another way is not supported.

*For SCM 2000, see the [Scalability](#) section for more information.*

<table>
<thead>
<tr>
<th>Feature</th>
<th>SCM 10 - 100</th>
<th>SCM 250 - 500</th>
<th>SCM 1000 - 2000*</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Quad-core processor or better</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard drive space</td>
<td>10 GB minimum</td>
<td>20 GB minimum</td>
<td>40 GB minimum</td>
</tr>
<tr>
<td></td>
<td>20 GB recommended</td>
<td>40 GB recommended</td>
<td>100 GB recommended</td>
</tr>
<tr>
<td>Memory</td>
<td>6 GB minimum</td>
<td>8 GB minimum</td>
<td>16 GB minimum</td>
</tr>
<tr>
<td></td>
<td>8 GB recommended</td>
<td>16 GB recommended</td>
<td>32 GB recommended</td>
</tr>
</tbody>
</table>

---

**Orion database server requirements**

The following table lists software and hardware requirements for your SolarWinds Orion database server using SCM license levels. You **must** create the SolarWinds Orion database with the SolarWinds Configuration Wizard. Creating the database another way is not supported.

*For SCM 2000, see the [Scalability](#) section for more information.*

<table>
<thead>
<tr>
<th>Feature</th>
<th>SCM 10 - 100</th>
<th>SCM 250 - 500</th>
<th>SCM 1000 - 2000*</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Quad-core processor or better</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard drive space</td>
<td>10 GB minimum</td>
<td>20 GB minimum</td>
<td>40 GB minimum</td>
</tr>
<tr>
<td></td>
<td>20 GB recommended</td>
<td>40 GB recommended</td>
<td>100 GB recommended</td>
</tr>
<tr>
<td>Memory</td>
<td>6 GB minimum</td>
<td>8 GB minimum</td>
<td>16 GB minimum</td>
</tr>
<tr>
<td></td>
<td>8 GB recommended</td>
<td>16 GB recommended</td>
<td>32 GB recommended</td>
</tr>
</tbody>
</table>

---

**Type**

**Language**

SolarWinds supports using SCM with database servers set up in the following languages:

- English
- German
- Japanese
- Chinese
<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>SolarWinds supports Express*, Standard, or Enterprise versions of the following:</td>
</tr>
</tbody>
</table>

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016 and SQL Server 2016 with SP1-SP2
- SQL Server 2014 and SQL Server 2014 with SP1-SP2
- SQL Server 2012**

*Microsoft SQL Server Express is suitable for up to SCM100 license tier. To reduce disk utilization when using SQL Server Express, shorten the Detailed Statistic Retention period on the Polling Settings page. The default value is 7 days. See [Optimize the database used by Orion Platform products](#), and see [Additional database space requirements](#) for more information on how much data can be consumed over time.

**Support for SQL Server 2012** is included in SCM 2020.2 so SCM 1.0 customers can upgrade to the latest version of SCM. For the best experience, use SQL Server 2016 or later.

- SCM local SQL database uses SQL 2017 EE Advanced by default.

- SolarWinds recommends that you use Express versions only for evaluations and very small environments.

### Recommendations

- Use the 64-bit version of SQL Server.
- Use the Simple database recovery mode to ensure best performance.
- You can set the database recovery model to Full Recovery if your Orion database is hosted on a SQL Cluster or if you use Always On Availability. However, you must back up your database regularly and ensure that the volume where you store your transactions log has free space equal to or greater than the size of the Orion database. Transaction logs will continue to grow indefinitely until a database backup is performed and transactions are committed to the database. SolarWinds recommends daily database backups if using the Full Recovery model.

You can use the following database select statement to check your SQL Server version, service pack, or release level, and edition:
<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server collations</td>
<td>The following SQL server collations are supported:</td>
</tr>
<tr>
<td></td>
<td>- English with collation setting SQL_Latin1_General_CP1_CI_AS</td>
</tr>
<tr>
<td></td>
<td>- German with collation setting German_PhoneBook_CI_AS</td>
</tr>
<tr>
<td></td>
<td>- Japanese with collation setting Japanese_CI_AS</td>
</tr>
<tr>
<td></td>
<td>- Simplified Chinese with collation setting Chinese_PRC_CI_AS</td>
</tr>
<tr>
<td></td>
<td>SolarWinds supports a case insensitive (CI) database on a CS SQL Server.</td>
</tr>
<tr>
<td></td>
<td>SolarWinds products do not support case-sensitive databases.</td>
</tr>
<tr>
<td>x86 components</td>
<td>The following x86 components must be installed:</td>
</tr>
<tr>
<td></td>
<td>- SQL Server System Common Language Runtime (CLR) Types</td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server Native Client</td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server Management Objects</td>
</tr>
<tr>
<td></td>
<td>If the components are not found on the target computer, the Orion Installer downloads and installs the components.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>SCM 10 -</th>
<th>SCM 250 -</th>
<th>SCM 1000 -</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SCM 100</td>
<td>SCM 500</td>
<td>SCM 2000*</td>
</tr>
<tr>
<td>CPU</td>
<td>Quad-core processor or better</td>
<td>2 x quad-core processor or better</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB minimum</td>
<td>16 GB minimum</td>
<td>64 GB minimum</td>
</tr>
<tr>
<td></td>
<td>16 GB recommended</td>
<td>64 GB recommended</td>
<td>128 GB recommended</td>
</tr>
<tr>
<td>Type</td>
<td>Requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard drive space</td>
<td>20 GB minimum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>100 GB minimum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 GB minimum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The amount of space needed by SCM depends on several variables in your environment. See <a href="#">Additional database space requirements</a> for details.</td>
<td>50 GB recommended</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>250 GB recommended</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>500 GB recommended</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SolarWinds database, data, and log files with a dedicated drive for the server OS and tempdb files.
- Other RAID configurations can negatively affect SQL Server performance.
- Mirrored drives for the OS and RAID 1+0 for database data files are recommended.
- Solid state drives (SSDs) are recommended for all components.

Some common files may need to be installed on the same drive as your server operating system. You may want to move or expand Windows or SQL temporary directories.

| Authentication     | Either mixed-mode or Windows authentication. If you require SQL authentication, you must enable mixed mode on your SQL server. |

| Other software | SolarWinds recommends installing the SQL Server Management Studio component on your Orion database server. |

The Orion Installer adds the following x86 components if they are not found on the Orion database server:

- SQL Server System Common Language Runtime (CLR) Types. Orion Platform products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance.
- Microsoft SQL Server Native Client
- Microsoft SQL Server Management Objects

For remote execution of PowerShell scripts, PowerShell 2.0 or later is required on the Orion server, Additional Polling Engines, and target servers.

**You cannot share the SolarWinds Orion database with Microsoft SharePoint, Microsoft Exchange, or BlackBerry servers.**

*For SCM 2000, see the [Scalability](#) section for more information.*

**SolarWinds recommends the following hard drive configuration:**
- A hardware RAID Controller with a battery backed-up write back cache
- Disk Subsystem 1 Array 1: 2x 146 GB 15K disks RAID 1 (mirroring) for the OS
- Disc Subsystem 2 Array 2: 2x 146 GB 15K disks RAID 1 (Pagefile + Extra Storage)
- Disk Subsystem 3 Array 3: with 6x 15K 146 GB or 300 GB disks configured in a RAID 1+0 array for SQL MDF and FILEGROUPS
- Disk Subsystem 4 Array 4: with 4x 15K 146 GB or 300 GB disks configured in a RAID 1+0 array for a SQL LDF Transaction LOG file
- Disk Subsystem 5 Array 5: with 4x 15K 146 GB or 300 GB disks configured in a RAID 1+0 array for a tempdb data file
- Disk Subsystem 6 Array 6: with 4x 15K 146 GB or 300 GB disks configured in a RAID 0 array for a tempdb log file

**Microsoft Azure deployments**

To deploy your Orion Platform product on Microsoft Azure, consider using the following instance types detailed in the table below, listed according to SCM license levels. For Microsoft Azure Managed Instance deployments, which SCM also supports, see the [Orion Platform system requirements](#).

<table>
<thead>
<tr>
<th>Requirements</th>
<th>SCM 10 - SCM 100</th>
<th>SCM 250 - 500</th>
<th>SCM 1000 - SCM 2000*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orion server</td>
<td>DS12_v2</td>
<td>DS12_v2</td>
<td>DS12_v2</td>
</tr>
<tr>
<td></td>
<td>4 CPU</td>
<td>4 CPU</td>
<td>4 CPU</td>
</tr>
<tr>
<td></td>
<td>16 GB RAM</td>
<td>16 GB RAM</td>
<td>16 GB RAM</td>
</tr>
<tr>
<td></td>
<td>150 GB disk</td>
<td>150 GB disk</td>
<td>150 GB disk</td>
</tr>
</tbody>
</table>
## Requirements

<table>
<thead>
<tr>
<th>SolarWinds Orion database server in an Azure VM</th>
<th>SCM 10 - SCM 100</th>
<th>SCM 250 - 500</th>
<th>SCM 1000 - SCM 2000*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DS4_V2 Standard</strong></td>
<td><strong>r4.D12_v2</strong></td>
<td><strong>D4_v2</strong></td>
<td><strong>Azure Storage Disk with Provisioned IOPS recommended</strong></td>
</tr>
<tr>
<td><strong>8 CPU</strong></td>
<td><strong>4 CPU</strong></td>
<td><strong>8 CPU</strong></td>
<td></td>
</tr>
<tr>
<td><strong>28 GB RAM</strong></td>
<td><strong>30.5 GB RAM</strong></td>
<td><strong>61 GB RAM</strong></td>
<td></td>
</tr>
<tr>
<td>System SSD 126 GB (included in Azure VM instance) + 1 TB for SQL database (included in Azure SQL Server Computer)</td>
<td>System SSD 80 GB (included in D12_v2) + Data Azure Storage Disk Volume 500 GB**</td>
<td>System SSD 160 GB (included in D4_v2) + 1x Data EBS Volume 150 GB + 2x Data Azure Storage Disk Volume 500 GB**</td>
<td></td>
</tr>
</tbody>
</table>

### SolarWinds Orion database using Azure SQL database

<table>
<thead>
<tr>
<th>DTU Standard Tier***</th>
<th>S3 (100 DTU)</th>
<th>S3 (100 DTU)</th>
<th>S4 (200 DTU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTU Premium Tier</td>
<td>P1 (125 DTU)</td>
<td>P1 (125 DTU)</td>
<td>P2 (250 DTU)</td>
</tr>
<tr>
<td>vCore General Purpose Tier</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>vCore Business Critical Tier</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Important:** SCM 2020.2 must run on Orion Platform 2020.2. The time zone setting of the Orion Server must be in the same time zone as the Azure SQL DB time zone (UTC).

When deploying Azure SQL and creating a new user in the Configuration wizard, SA account credentials are required.

---

When using Azure SQL for your database server, required tiers depend on whether you’re using memory-optimized tables (In-Memory OLTP) supported in SQL Server 2016 and 2019 to improve the performance of transaction processing, data ingestion, data load, and transient data scenarios.
<table>
<thead>
<tr>
<th>Requirements</th>
<th>SCM 10 - SCM 100</th>
<th>SCM 250 - 500</th>
<th>SCM 1000 - SCM 2000*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure SQL tiers if using In-Memory OLTP</strong></td>
<td>DTU Tier P1</td>
<td>DTU Tier P2</td>
<td>DTU Tier P4</td>
</tr>
<tr>
<td></td>
<td>vCore Business</td>
<td>vCore Business</td>
<td>vCore Business</td>
</tr>
<tr>
<td></td>
<td>Critical Gen4 Tier 1</td>
<td>Critical Gen4 Tier 2</td>
<td>Critical Gen4 Tier 4</td>
</tr>
<tr>
<td></td>
<td>vCore Business</td>
<td>vCore Business</td>
<td>vCore Business</td>
</tr>
<tr>
<td></td>
<td>Critical Gen5 Tier 2</td>
<td>Critical Gen5 Tier 2</td>
<td>Critical Gen5 Tier 4</td>
</tr>
<tr>
<td><strong>Azure SQL tiers without In-Memory OLTP</strong></td>
<td>DTU Tier S3</td>
<td>DTU Tier S3</td>
<td>DTU Tier S4</td>
</tr>
<tr>
<td></td>
<td>DTU Premium Tier P1</td>
<td>DTU Premium Tier P1</td>
<td>DTU Premium Tier P2</td>
</tr>
<tr>
<td></td>
<td>vCore General Purpose Tier 2</td>
<td>vCore General Purpose Tier 2</td>
<td>vCore General Purpose Tier 2</td>
</tr>
<tr>
<td></td>
<td>vCore Business</td>
<td>vCore Business</td>
<td>vCore Business</td>
</tr>
<tr>
<td></td>
<td>Critical Tier 2</td>
<td>Critical Tier 2</td>
<td>Critical Tier 2</td>
</tr>
</tbody>
</table>

*For SCM 2000, see the [Scalability](#) section for more information.*

**Azure Storage Disk volumes are not your dedicated hardware. Consider using Azure Reserved Instances of storage disk volumes for SQL servers.**

***SolarWinds recommends that customers with large environments or environments with frequent changes use DTU Premium Tier, vCore General Purpose Tier, or vCore Business Critical Tier (rather than DTU Standard Tier), as these tiers allow more IOPS.***
Additional database space requirements

The amount of space required by SCM depends on the number of nodes being monitored, the frequency of changes, the number of configuration items being monitored, and the average size of a configuration item. Use the following examples to help determine your needs.

<table>
<thead>
<tr>
<th>Number of nodes monitored by SCM</th>
<th>Number of configuration items per node</th>
<th>Average size of configuration item</th>
<th>Frequency of changes</th>
<th>Additional database space recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>100</td>
<td>10.00 kB</td>
<td>Once per week, every item changes</td>
<td>52 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Once per day, every item changes</td>
<td>365 GB</td>
</tr>
<tr>
<td>50</td>
<td>100</td>
<td>10.00 kB</td>
<td>Once per week, every item changes</td>
<td>26 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.00 kB</td>
<td></td>
<td>13 GB</td>
</tr>
</tbody>
</table>

SCM database monitoring requirements

Starting with SCM 2020.2, an ODBC driver is required. Drivers are automatically installed along with SCM. The following database versions can be monitored via out-of-the-box profiles using SCM:

- MS SQL versions 2012 and later
- MySQL versions:
  - 5.7
  - 8.0
- PostgreSQL versions:
  - 9.4.25
  - 9.5.20
  - 9.6.16
  - 10.11
  - 11.6
  - 12.1
There are no specific permissions needed by SCM for polling out-of-the-box database profiles. What is polled depends on what the user enters into the connection string field. SolarWinds recommends that you enter macros in the connection string to make use of credentials stored in the Orion Platform. If credentials are entered directly into the connection string, they are stored in plaintext.

**Scalability**

An Orion instance with SCM installed can process up to 280 changes/second combined. If you expect to have more than 1,000 agents per polling engine, you will need an Additional Polling Engine (APE).

> See also [Scalability Engine Guidelines for SolarWinds products](#).

Adding an APE enables you to collect data at a rate or volume beyond the capacity of a single SCM server. You can also use APEs for organizational purposes, so server configurations at each specific site are monitored by site-specific APEs.

APEs are already included with your SCM license. Therefore, you can have as many SCM-specific APEs as you need, and you don't need to purchase any additional licenses. To set up an APE for SCM, you just need to select the option Additional Polling Engine for Server Configuration Monitor when you install the APE using the SolarWinds Orion Installer.

> By selecting Additional Polling Engine for Server Configuration Monitor during the installation of an APE, that included APE can poll only servers that are monitored with SCM or other products specifically mentioned as compatible with the APE during the installation.

**More learning resources**

To learn more about Orion Platform requirements and configurations, refer to:

- [Orion Agent requirements](#)
- [High Availability requirements](#)
- [Port requirements for all SolarWinds products](#)
- [Deploy Orion Platform products to Microsoft Azure](#)
- [Multi-module system guidelines](#)
- [Scalability Engine Guidelines for Orion Platform products](#)
- [Orion Platform Optimization Guide](#)
SCM licensing model

SCM is licensed per node. A node counts toward your total while it has at least one SCM profile assigned to it.

Orion Platform products support both perpetual licenses and subscription licenses. See License types in the Orion Platform help for details.

The following SCM license tiers are available:

<table>
<thead>
<tr>
<th>License Tier</th>
<th>Number of Managed Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCM10</td>
<td>10</td>
</tr>
<tr>
<td>SCM25</td>
<td>25</td>
</tr>
<tr>
<td>SCM50</td>
<td>50</td>
</tr>
<tr>
<td>SCM100</td>
<td>100</td>
</tr>
<tr>
<td>SCM250</td>
<td>250</td>
</tr>
<tr>
<td>SCM500</td>
<td>500</td>
</tr>
<tr>
<td>SCM1000</td>
<td>1000</td>
</tr>
<tr>
<td>SCM2000</td>
<td>2000</td>
</tr>
</tbody>
</table>
Node management

Nodes supported by Server Configuration Monitor (SCM)

Server Configuration Monitor supports monitoring on Windows-based devices, and beginning with SCM 2019.4, Linux machines with Linux kernel 2.6.23 or later. Monitoring profiles that include file or registry elements require that the device be polled by the Orion Agent for Windows on Windows Server 2008 R2 SP1 or later. The out-of-the-box HW and SW inventory profiles require Asset Inventory, which can be enabled through List Resources on the Node Details page.

Add a node to SCM

To add servers already monitored by the Orion Platform to Server Configuration Monitor (SCM), start configuration monitoring on the device.

To monitor servers using SCM, you must first add them to the Orion Platform. There are several ways to add devices to the Orion Platform, but the following ways allow you to start SCM monitoring at the same time:

- Add a node through Network Discovery
- Add a node through the Add Node wizard

To learn more about adding nodes to the Orion Platform, see the Orion Platform Administrator Guide.

Add a node to Server Configuration Monitor (SCM) through Network Discovery

1. In the Orion Web Console menu, navigate to Settings > Network Discovery.
2. Click Add New Discovery, and then click Start.
3. On the Network panel, if this is your first discovery, add a limited number of IP addresses.

As you scale your implementation, you can use the following scanning options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Ranges</strong></td>
<td>Use this option when you want Orion to scan one or more IP ranges. If you have many IP ranges to scan, consider adding multiple discovery jobs rather than including all ranges in a single job.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td>Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (512 addresses max). Scanning a subnet returns everything that responds to ping, so we recommend scanning subnets only where the majority of devices are objects you want to monitor.</td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
<td>Use this option for a limited number of IP addresses that do not fall in a range. Since a network discovery job can take a long time to complete, SolarWinds recommends using this option when you are first starting out.</td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
<td>Use this option to scan an Active Directory Domain Controller. Using Active Directory for discovery is particularly useful for adding large subnets because Orion can use the devices specified in Active Directory instead of scanning every IP address.</td>
</tr>
</tbody>
</table>
4. If the Agent panel is displayed, you enabled the Quality of Experience (QoE) agent during installation. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes check box. Click Next.

This setting ensures that any agents you deploy, including the one on your Orion server, are up to date. If there are no nodes using agents, you can leave this option unchecked.

5. On the SNMP panel:

a. If all devices on your network require only the default SNMPv2 public and private community strings, click Next.

b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required
information. Click Add, and then click Next.

6. On the Windows panel, to discover WMI or RPC-enabled Windows devices, click Add New Credential and provide the required information. Click Add, and then click Next.

To monitor for configuration changes on Windows, you must deploy an agent.
7. On the Monitoring Settings panel, you can choose to manually set up monitoring the first time you run discovery, or you can automatically monitor based on settings that you define.

   a. To manually set up monitoring after devices are discovered, click Manually set up monitoring after devices are discovered, and then click Next.
b. To define monitoring settings and then automatically monitor based on those settings, click Automatically monitor based on my defined settings, and then click Define monitoring settings. Click Next.
Select the Volume Types to monitor, and then click Next.
Hardware and software inventory are automatically assigned for nodes with enabled Asset Inventory, and the IIS profile is assigned when IIS is detected on a node.

Select the server configuration profiles to monitor, or if you prefer not to automatically assign profiles to newly discovered nodes, deselect any or all of the profile types. Click Finish, and then click Next.
Only out-of-the-box profiles can be added this way. Selected profiles will be applied to all discovered nodes that are eligible for that type of monitoring. This eligibility is determined by the presence of specific files or registries on the node. For example, IIS configuration files must be present for the IIS profile to be applied. Profiles other than hardware and software inventories require polling via an Orion Agent for Windows or Linux.

8. On the Discovery Settings panel, click Next.
9. Accept the default frequency and click Discover to run discovery immediately.

![Network Sonar Wizard]

Discovery can take anywhere from a few minutes to a few hours, depending on the number of network elements the system discovers.

![DISCOVERING NETWORK...]

10. After discovery has completed:
    a. If you defined your monitoring settings above, this procedure is complete, and your results are displayed.
    b. If you chose to manually set up monitoring after devices are discovered, select the device types to import, and click Next.

![Network Sonar Results Wizard]

Select the volume types to import, and click Next.
Select the server configuration profiles to import, and then click Next.

Select the devices and volumes you want to import (or ignore), and then click Import (or Ignore).

Then click Finish.
Your results are displayed.

Add a node to Server Configuration Monitor (SCM) through the Add Node wizard

1. In the Orion Web Console menu, navigate to Settings > Manage Nodes.
2. Click Add Node.
3. Specify the node, and click Next.
   a. Provide the host name or IP address.
   b. Select the polling method, and provide credentials.

   ▪ Most SCM monitoring requires polling via an Orion Agent for Windows or Linux.

4. In the Choose Resources step, select the profiles you would like to monitor under Server Configuration. Click Next.

   ▪ Only out-of-the-box profiles can be assigned this way. To assign custom profiles, see Assign configuration profiles to a node.

5. Review and adjust the device properties. Click OK, Add Node.
See nodes monitored by Server Configuration Monitor (SCM)

All users can see the nodes currently being monitored by SCM in the Server Configuration Nodes widget on the Server Configuration Summary page. The Server Configuration Summary page can be found under My Dashboards.

Users with the SCM Admin role can also see the Monitored Nodes section of Server Configuration Monitor Settings:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings and selecting Server Configuration Monitor Settings under Product Specific Settings.

2. Click the Monitored Nodes tab in the upper left.

From here, you can assign and unassign profiles from the nodes that are already being monitored.

Understand updates to asset inventory discovery in SCM

Prior to the release of Server Configuration Monitor (SCM) 2019.4, when a new installation of SCM brought asset inventory into the Orion server, asset inventory was automatically enabled for all eligible nodes, with the exception of agent nodes. But starting with SCM 2019.4, when any newly installed module brings asset inventory into the Orion server, asset inventory is automatically enabled for all eligible nodes, including agent nodes.

When you click Add Agent on the Manage Agents page to create a new node, asset inventory for the node is discovered in the background and enabled when applicable. However, you can opt out of the feature in Advanced Configuration via settings, EnableAgentAutomaticDiscovery.

User restrictions in Server Configuration Monitor (SCM)

In order to make changes to profiles, profile assignments, and data retention settings in Server Configuration Settings, a user must have the SCM role Admin and node management rights. These permissions can be granted or revoked through Manage Accounts.
Monitor configuration changes on a node in SCM

In Server Configuration Monitor (SCM), set up configuration monitoring on a server, see suggestions of servers to monitor, and see the recent changes.

This assumes you have already added the node to the Orion Platform. See Add a node to SCM for details.

To begin monitoring server configurations, you must assign one or more configuration profiles to the server.

- Assign configuration profiles to a node
- Unassign configuration profiles
- See detected candidates for configuration monitoring
- Monitor Linux nodes in SCM
- Monitor file attributes in SCM
- Monitor a SQL database in SCM
- Understand database queries in SCM
- Learn about near real-time change detection
- Monitor who made server configuration changes
- Enable near real-time file monitoring
- See recent configuration changes
- Enable out-of-the-box monitoring exclusions
- Take advantage of SCM PowerShell script support
- Leverage Linux scripts
- Test SCM profile elements before deploying them
- Change how long configuration data is kept
- Watch for specific configuration changes
- View the structural diff in SCM

Assign configuration profiles to a node in Server Configuration Monitor (SCM)

This task is not available to all users. See User restrictions for details.

To begin monitoring server configurations, you must assign one or more configuration profiles to the server. There are multiple ways to assign configuration profiles:
Through Server Configuration Monitor Settings

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor settings under the Product Specific Settings heading.

2. Pick either the Profiles tab or the Monitored Nodes tab. If you need to assign profiles to a node that is not already in SCM, choose Monitored Nodes.
   a. From Profiles:
      i. Select the profiles to assign, and click Assign To in the ribbon.
ii. Choose the nodes to assign the profiles to, then click Next.

iii. If you are required to set credentials (for database elements) or want to set optional credentials for other types of elements such as file elements, registry elements, or script elements, do so by following the prompts to set credentials.
Assign configuration profiles

Set credentials

Set credentials required by specific element types. If desired, set additional credentials as well. If you need more granular credentials settings, set them later on the Assigned elements page.

DATABASE QUERY: 31 elements found in 1 profile

Connection string

Select existing connection string or add new one...

Pick the connection string that matches the database type you want to monitor. You can use the following macros: $1(NodeIP), $2(NodeFqdn), $3(Username), and $4(Password). These macros will be substituted with the appropriate values during execution. Windows authentication is not supported, so you must provide database account credentials. Learn more about database queries

Credentials

Select existing credentials or add new ones...

or
b. From Monitored Nodes:

   i. Select the node(s) to assign profiles to from the list of nodes already in SCM, then choose Assign Profiles.
   
   If you do not see the node you want to assign profiles to, click Set Up Configuration.
Monitoring to add a new node to SCM.
ii. Select the profiles to assign, then click Next.

iii. If you are required to set credentials (for database elements) or want to set optional credentials for other types of elements such as file elements, registry elements, or script elements, do so by following the prompts to set credentials.
Assign configuration profiles

Set credentials

Set credentials required by specific element types. If desired, set additional credentials as well. If you need more granular credentials settings, set them later on the Assigned elements page.

DATABASE QUERY: 25 elements found in 1 profile

Connection string

Select existing connection string or add new one...

Pick the connection string that matches the database type you want to monitor. You can use the following macros: $[Node], $[Nodehostname], $[Username], and $[Password]. These macros will be substituted with the appropriate values during execution. Windows authentication is not supported, so you must provide database account credentials. Learn more about database queries.

Credentials

Select existing credentials or add new ones...

or

SET ADDITIONAL CREDENTIALS

ELEMENT TYPE

File

Linux script

< BACK NEXT CANCEL
3. Review the assignments on the summary page. Here you will see warnings if there are any potential polling issues detected, such as Asset Inventory being disabled on a node when assigning a profile that requires it. You can still assign profiles if a warning occurs, but SCM will
not start collecting that data until the conflict is resolved. You also have the option to re-check problems and click Confirm to finish the assignment.

**Through List Resources**

**Out-of-the-box profiles** can be assigned through a node’s List Resources.

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.

2. Under Server Configuration, select the profiles you want to assign or unassign.
   
   Custom profiles are not included in List Resources.

3. Click Submit to save your changes.

**From the Server Configuration Summary page**

Custom and out-of-the-box profiles can be assigned from the Server Configuration Summary page.
1. Navigate to My Dashboards > Server Configuration Summary.

2. In the Server Configuration Nodes widget, click Assign Configuration Profiles, or in the Candidate for Server Configuration Monitoring widget, click Assign profile to assign a profile to a node.

3. Select the profiles you wish to assign, then click Next.

4. Select the nodes to which those profiles should be assigned, then click Next. The list of nodes can be filtered by node properties, including custom properties.

5. If needed or desired, set credentials.

6. Review the profile assignments, then click Confirm to finish the profile assignments. Be sure to note potential errors that are indicated, including unsupported node assignments or improper combinations of profiles and nodes.

**Assign or unassign from the Manage Nodes page**

You can assign a profile to a selected node or unassign a profile from a selected node directly from the Manage Nodes page in Server Configuration Monitor (SCM). There is also an optional column on the Manage Nodes grid so you can view which profiles are assigned to selected nodes.
Unassign configuration profiles in Server Configuration Monitor (SCM)

This task is not available to all users. See User restrictions for details.

There are two ways to unassign configuration profiles:

Through Server Configuration Monitor Settings

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Switch to the Monitored Nodes tab.
3. Select the node(s) you want to unassign profiles from.
4. Click Unassign Profiles on the ribbon.
5. Select the profiles you want to unassign, then click Unassign.
6. You will be prompted with a question about keeping historical data. You can choose to keep the data SCM has collected from the unassigned profiles if you would like to see that information when looking at the configuration history. If you choose to delete the data, that history will be gone. Click either Keep Data or Delete Data to finish the unassignment.

Through List Resources

Out-of-the-box profiles can be unassigned through a node’s List Resources. There is no option to keep the historical data if unassigning profiles this way.

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.
2. Under Server Configuration, select the profiles you want to assign or unassign.
   - Custom profiles are not included in List Resources.
3. Click Submit to save your changes.
You may want to assign the same profile(s) to multiple servers. Instead of assigning and unassigning each profile individually, you can assign and unassign profiles in bulk.

From the Manage Nodes page

See instructions for unassigning configuration profiles from the Manage Nodes page.

See detected candidates for configuration monitoring in Server Configuration Monitor (SCM)

SCM will automatically detect servers that have been added to the Orion Platform that might be eligible for monitoring one or more of the out-of-the-box profiles. You can view a list of candidate servers on the SCM Summary page, which can be found under My Dashboards.

The Candidates for Server Configuration Monitoring widget lists servers that might be eligible for configuration monitoring but do not have an agent, and servers that are eligible for monitoring each out-of-the-box profile. From there, you can push agents or assign the suggested profiles using the links provided. The Dismiss all link will stop those nodes from being suggested again.

Whether a node is eligible for configuration monitoring is determined in the following ways:

<table>
<thead>
<tr>
<th>Suggested action</th>
<th>Eligibility requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push an agent</td>
<td>Any node running Windows Server 2008 R2 SP1 or later</td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>Any node running Linux kernel 2.6.23 or later</td>
</tr>
<tr>
<td>Assign HW/SW inventory profiles</td>
<td>Any node with AssetInventory enabled</td>
</tr>
<tr>
<td>Assign an out-of-the-box profile</td>
<td>If the node is monitored by a respective SAM application, it’s a candidate for SCM monitoring by a specific profile. For example, any node monitored by AppInsight for IIS, or another SAM app template tagged as 'IIS' is a candidate for SCM monitoring by IIS configuration profile.</td>
</tr>
</tbody>
</table>
Monitor Linux nodes in SCM

Starting with Server Configuration Monitor (SCM) 2019.4, you can monitor Linux nodes via Orion agent. Just as on Windows nodes, the SCM agent plugin must be installed on monitored nodes to monitor files, and the Asset Inventory agent plugin is required for HW and SW inventory profiles. Linux machines with Linux kernel 2.6.23 or later are supported.

The Orion agent runs under the swiagent user. For more information about the Orion agent, see SolarWinds Orion agent requirements.

To monitor your Linux environment, see this page for instructions on how to configure SNMP for agents deployed by SCM. (These instructions apply to SAM, SCM, and other products.) Once installed, it should auto-configure for you.

Monitor Linux files

The dialog for adding file elements remains the same, using the generic File profile elements. SCM automatically distinguishes between files with Linux filepaths, such as /etc/init.d/*.config and Windows filepaths, such as C:\Program Files\Solarwinds\*.config. You can monitor individual files or use wildcard characters to dynamically monitor any sub-directory and file. SCM also supports Linux system variables such as ${HOME}.
The polling is interval-based. The polling frequency setting is shared with Windows file polling.

Monitor hardware and software

Monitoring hardware and software inventory also works on Linux machines via the Asset Inventory Linux agent plugin.
Execute Linux scripts (bash, python, or others)

You can define custom Linux scripts in SCM to capture any desired output that meets your business needs. The Linux script element enables you to run scripts in any language that is available on the monitored system. It is executed using the swiagent account. Optionally, you may specify script content that is stored in a temporary file. The file can then be referenced in the command line with the `${Script-file}` macro. The output of this script is then collected and used for change detection in the same way the PowerShell script element is. This provides readily available business data analysis and enables you to manage your Linux scripts from on location. To learn more about Linux scripts, see Leverage Linux scripts in SCM.

Monitor file attributes in SCM

In addition to monitoring file metadata such as last modification time, size, and file owner, Server Configuration Monitor (SCM) now monitors even more file attributes. For file elements only, on both Windows and Linux, SCM can now capture permissions, user access read and write information, and various other attributes that tell you about the files.

Tracking these attributes is useful in a number of ways, including improving your ability to detect intrusion attempts. For instance, a bad actor could make a change to a file’s permissions so that you cannot easily see the changes they make to a file. By viewing the file attribute changes, you can see that file permissions were changed, and you can take action to stop unwanted changes to your files.

When file attributes change, a new version is created, and the version is timestamped as the 'Last change detected' in the Configuration details resource. The following are examples of file attribute changes on both Windows and Linux machines that can be viewed on the Content Comparison page:
Monitor a SQL database with SCM

You can now monitor databases for changes using Server Configuration Monitor (SCM), by running SQL queries to connect to any relational database such as Microsoft SQL Server, PostgreSQL, Oracle, or MySQL. SCM can collect data through SQL queries, then store that data and watch it for changes. This process enables SCM to track and alert you to changes made to user permissions, tables, indexes, views, stored procedures, scheduled jobs, and any other data you can gather using SQL queries.
Monitoring databases in SCM does not require an agent and can be performed on any type of node (Agent, WMI, SNMP, ICMP, and external). You must provide database account credentials required to monitor databases. Windows authentication is not supported. Along with supporting the use of credentials for databases, you can now add credentials for scripts and files. For more information on using credentials in SCM, see Specify element credentials in SCM.

Set up and install

To monitor a SQL element with Server Configuration Monitor (SCM), follow these instructions.

1. Ensure that you can connect to the SQL database and that your SQL server is set to allow remote connections.

2. The ODBC drivers are automatically installed with SCM 2020.2 or later unless FIPS is enabled on the system.

Configure SCM to monitor a Database query element

1. Open SCM and go to the Server Configuration Monitor Settings page.

2. Click the Profiles tab, and create new or edit an existing profile with a Database Query Element to test connectivity.
3. Select, modify, or create a new connection string using the drop-down menu.

4. Fill in or edit the element with the database query you want to test or that is collecting the desired configuration data.
5. Specify SQL credentials and click TEST to test the connection.

Note: Due to security concerns, SolarWinds recommends that you avoid using username and password values in the Connection String. Instead, use the \$\{username\} and \$\{password\} macros along with specified credentials to ensure that sensitive values are properly secured.

6. Select the node you want to test.
7. After following these steps, the test should be successful. The success of the test is indicated on your test results page.

![Test Results](image)

However, if there is an issue, an error message is displayed to help you start troubleshooting.

![Error Message](image)

**Out-of-the-box database profiles**

There are new out-of-the-box profiles available to help you maximize this functionality:

- MS SQL Server
- PostgreSQL
- MySQL

These out-of-the-box profiles provide a starting point for you to start monitoring your databases, and they can be customized to meet your organization's needs.

**Additional notes on database monitoring**

Users should take note of the following:

- The SQL element in SCM can use only 32-bit ODBC drivers to connect to a database. This is not an issue for the databases, which use ODBC drivers provided by SolarWinds. However, if you use different drivers that are 64-bit, they would not work.

- If you choose the *Use Orion default credentials needed* option and enter your login directly into the connection string, your credential information will be stored in the database in plaintext. Therefore, SolarWinds recommends that you use ${Username} and ${Password} macros and use credentials that are stored in the Orion Platform.

- ODBC drivers are not installed with SCM if you have FIPS enabled on your system.
Understand database queries in SCM

You can run SQL queries in Server Configuration Monitor (SCM) to connect to relational databases such as SQL Server, PostgreSQL, Oracle, and MySQL. When adding configuration elements for monitoring, there is now an option to choose the element type Database query. The connection string drop-down menu contains one example connection string for each pre-installed driver, and a list of all connection strings used in all elements. The following macros are available in the connection string:

- ${NodeIP} - IP address of polled database
- ${NodeHostname} - Hostname of polled database
- ${Username} - assigned credential username
- ${Password} - assigned credential password

The following is an example of a connection string:

```
Driver={MariaDB ODBC 3.1};Server=${NodeIP};User=${Username};Password=${Password};Option =3;Port=3306
```

Custom ODBC Drivers

You can poll the database with any other driver if you install it on the poller. Only 32-bit drivers are allowed because the process that it polls is a 32-bit process.

Learn about near real-time change detection in SCM

Server Configuration Monitor (SCM) offers near real-time change detection to provide a more granular representation of changes to your environment. Rather than a view of periodic, aggregated server configuration changes, SCM actively listens to identify and track changes to configurations as they occur. This enables SCM users to see the full spectrum of changes that occur between polling cycles so that they can proactively anticipate performance impacts.

The SCM agent plugin requires deployment of the File Integrity Monitor to monitored servers to enable the capture of any file change in near real time and to indicate who made the change. To use this feature, you must turn on near real-time file monitoring, which enables 'who made the change monitoring.' See the topic Enable near real-time file monitoring and 'who made the change' detection for instructions.

When near real-time monitoring is disabled:
File/parsed file elements use IntervalWatcher instead. Registry elements use RegistryWatcher instead.

When real-time monitoring is enabled:

- Parsed/file elements use the FIM driver, and 'who made the change' detection is enabled to show who made changes to server configurations.
- Registry elements use the FIM driver, and 'who made the change' detection is enabled to show who made changes to server configurations.

**Monitor who made server configuration changes using SCM**

Server Configuration Monitor (SCM) comes with a 'who made the change' detection capability to monitor who made server configuration changes. To use this feature, you must turn on near real-time file monitoring, which enables 'who made the change monitoring.' See the topic [Enable near real-time file monitoring and 'who made the change' detection](#) for instructions.

There are some limitations to the 'who made the change' functionality, which are described below, along with the messages a user may encounter in SCM when the 'who' value cannot be detected.

**When is 'who made the change' detection available?**

Consult the following table to determine when 'who made the change' detection is available.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Agent-less</th>
<th>Via agent</th>
<th>Supports 'Who made the change' detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Software</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Registry</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(Windows only)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Files</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux files</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PowerShell</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Linux script</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Database</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

In addition, the following conditions affect 'who made the change' data:

- Historical data is lost if you switch the collection of hardware and software data between remote and agent.
• When looking at the profile, the 'who' value is displayed only when the most recent change is from an element that supports collecting 'who' information.
Messages displayed when the 'who' value is not available

<table>
<thead>
<tr>
<th>Message Displayed in SCM</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The 'who' value is not available because this change event was not captured in time. Learn more.</td>
<td>SCM cannot determine 'who' made the change, as this change was not detected at the exact time it occurred. For example, the change was detected:</td>
</tr>
<tr>
<td></td>
<td>- After the node was remanaged.</td>
</tr>
<tr>
<td></td>
<td>- After the agent was restarted.</td>
</tr>
<tr>
<td></td>
<td>- When 'Poll Now' was triggered.</td>
</tr>
<tr>
<td>The 'who' value is not available because real-time change detection was disabled. Learn more.</td>
<td>The SCM polling method does not allow capture of 'who' made the change when real-time change detection is disabled.</td>
</tr>
<tr>
<td>The 'who' value is not available because more than one change was detected at the same time. Learn more.</td>
<td>When more than one change event is detected at the same time, SCM cannot determine the usernames associated with each change.</td>
</tr>
<tr>
<td>The 'who' value is not available because the changes were aggregated according to data retention settings. Learn more.</td>
<td>SCM cannot determine which username to associate with this change after changes are aggregated according to data retention settings.</td>
</tr>
<tr>
<td>The 'who' value is not available because this node is explicitly excluded from enhanced change detection. Learn more.</td>
<td>Even though global real-time polling is enabled, the selected node was specifically excluded from real-time polling in enhanced change detection settings. SCM does not collect the usernames associated with changes when real-time polling is not enabled.</td>
</tr>
</tbody>
</table>
Enable near real-time file monitoring and 'who made the change' detection in SCM

To enable near real-time file monitoring and 'who made the change' detection in Server Configuration Monitor (SCM), take the following steps:

1. Log into the Orion Web Console.
2. Click Settings > All Settings.
4. Select the Polling Settings tab, and at the right of your screen, click the switch to turn on 'Who made the change' detection.

5. Click Continue to Setup.
6. If there are nodes on which you do not want the FIM driver installed, you can exclude those nodes from near real-time monitoring and ‘who made the change’ detection by clicking Add exclusions. Then click Enable who detection.

See recent configuration changes in Server Configuration Monitor (SCM)

To see the most recent configurations from all monitored nodes, find the Recent Configuration Changes widget on the Server Configuration Summary dashboard.

This widget shows all configuration changes in the selected time interval. Each row shows the name of the profile in bold, the node the change was made on, and the element name/path. The color to the left of each entry indicates the type of change: yellow for addition, blue for an update, and red for removal. Clicking a row will take you to a comparison between the two most recent versions (see Compare configurations over time).

The initial poll is not included in the list of all configuration changes. The initial data is not considered a change, since there was no previous data to compare to.

To see the most recent configuration changes on a particular node, see the Recent Configuration Changes widget on the Server Configuration page of Node Details.
Enable out-of-the-box monitoring exclusions in Server Configuration Monitor (SCM)

Out-of-the-box profiles in SCM allow the ability to ignore specified changed values in SCM hardware or software inventory profiles using exclusion rules for common scenarios.

You may want to stop monitoring specific values in hardware and software monitoring, as those changes may represent false positives. For instance, you can:

- Exclude total memory from hardware inventory monitoring on virtual machine node types.
- Exclude any driver names that contain the word "Remote" from software inventory monitoring.

Exclusions can be applied only to profiles with SolarWinds Information Service (SWIS) query (internal query) elements.

To exclude hardware or software data from change detection, take one (but not both) of the following actions:

- Copy the out-of-the-box profile and edit the SolarWinds Information Service (SWIS) query directly.
- Create an exclusion rule directly in the database.

To copy an out-of-the-box profile in SCM:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab (if it is not selected by default).
3. Select the SW inventory profile, and then click Copy.
4. Rename the copied profile.
5. Edit the SWIS query in the new profile.
6. Save the new profile.

Copied profiles are a type of custom profile, so they are not displayed in List Resources. They are also not detected in Network Discovery and not displayed in the SCM candidates resource. Only out-of-the-box configuration profiles are detected there.

To create an exclusion rule in the database:

Use the database table (definition table [SolarWindsOrion].[dbo].[SCM_QueryElement_ExclusionRules]), and insert content manually as needed. See the example of the database table below that can be used to create the following exclusion rules:
- Exclude total memory from hardware inventory monitoring on virtual machine node types.
- Exclude any driver names that contain the word "Remote" from software inventory monitoring.
- Exclude any changes that relate to operating system update KB123 for Node 3.

The first two rules listed in the table below already exist in the database, but are not active. To activate one of these rules, use the following:

```
UPDATE [SolarWindsOrion].dbo.[SCM_QueryElement_ExclusionRules] SET Active = 1 WHERE ID=?
```

The third rule in the table below is an example of a rule that can be created, but it does not currently exist in the database.

Table name: [SolarWindsOrion].dbo.[SCM_QueryElement_ExclusionRules]

<table>
<thead>
<tr>
<th>NodeID</th>
<th>ProfileID</th>
<th>ElementDisplayAlias</th>
<th>ExclusionQueryWhereCond</th>
<th>ExcludedColumns</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL</td>
<td>2 (SW inventory)</td>
<td>Software Installed</td>
<td>WHERE Model = 'Virtual Machine'</td>
<td>TotalMemoryB;someOtherColumn</td>
<td>1</td>
</tr>
<tr>
<td>NULL</td>
<td>1 (HW inventory)</td>
<td>Drivers</td>
<td>WHERE NAME LIKE '%remote%'</td>
<td>NULL</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>OS Updates</td>
<td>WHERE Name = 'KB123'</td>
<td>NULL</td>
<td>1</td>
</tr>
</tbody>
</table>

- NULL in the NodeID column indicates that the exclusion rule is applied for all nodes.
- If ExclusionQuery fails, no exclusion is created, and an error message is displayed.

Scripts are not supported under any SolarWinds support program or service. Scripts are provided AS IS without warranty of any kind. SolarWinds further disclaims all warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The risk arising out of the use or performance of the scripts and documentation stays with you. In no event shall SolarWinds or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the scripts or documentation.
Take advantage of PowerShell script support in Server Configuration Monitor (SCM)

Created by Microsoft, PowerShell is a task automation and configuration management framework that consists of a command-line shell and associated scripting language, built on the .NET Framework.

Your organization should internally review and assess to what extent PowerShell is incorporated into your environment. This is especially important when importing scripts from third parties, including content posted by other customers in the SolarWinds online IT community, THWACK.

PowerShell does not process text; it processes objects based on the .NET Framework.

You can define custom PowerShell scripts in SCM to capture a wide range of different outputs according to your business needs. Create an SCM profile with the PowerShell script element and assign it to desired nodes. SCM then collects the output of those scripts and alerts you when it changes so that you can compare data outputs over time. This eliminates the need for manual data analysis and enables you to manage your PowerShell scripts from a central location, ensuring consistency throughout your environment.
SolarWinds recommends that you avoid using credentials or other sensitive information in PowerShell or Linux script content, as this information may be viewable by non-administrator SCM users.

A PowerShell script for an element cannot be executed more than once at the same time. Therefore, if the same script is started again while the PowerShell script is still running, the SCM agent plugin ignores the newer attempt at script execution and waits for the result of the currently running script instead. The frequency of change detection may be lowered to ensure that the target system is not exhausted due to a complicated script.

PowerShell script outputs automatically preserve 4,096 characters. If you have formatting issues, see Display of PowerShell output in SCM does not match console output.

**Leverage Linux scripts in SCM**

Linux script elements are available as part of out-of-the-box profiles and custom profiles, starting with Server Configuration Monitor (SCM) 2019.4. Collect an array of different outputs using custom Linux scripts in SCM to help you automate change detection and data interpretation. You can run scripts in any language available on the system you're monitoring. Scripts are executed using the swiagent account.

- Install and properly configure your script interpreter, and you may choose from a variety of different scripting languages to use in SCM, including bash, python, or perl.
- Element settings for Linux scripts in SCM apply in the same way they do for PowerShell scripts, and take into account timeouts and polling frequency.
- Agent must be installed and configured on Linux/Unix-based computers. During this process, a service account, swiagent, is created to run the agent service.

Test SCM profile elements before deploying them

Server Configuration Monitor (SCM) now features a TEST button for monitoring in the Add/Edit/View configuration element dialog box. Test any type of element to see whether it works on one of your monitored nodes before you deploy it to your servers.

1. To use the test function, add a configuration element for monitoring, and then select credentials from the drop-down menu under Access authentication.
2. After setting the credential, click TEST.

SCM displays a list of nodes on your machine from which you can choose. (In the following example, a Linux machine is selected, as the user wants to execute a bash command.)
3. Click Select & Test.

4. SCM displays your test result.

See the following example of a successful test result:

See the following example of a successful test result using a file wildcard definition that returned multiple configuration items:
See the following example of a failing test result:

![Test Result Example]

Change how long configuration data is kept in Server Configuration Monitor (SCM)

- **This task is not available to all users. See [User restrictions](#) for details.**
SCM retains configuration data at three levels of granularity: detailed, hourly, and daily. Detailed data is every change detected for every configuration item. Hourly data is the most recent change detected within the hour for each configuration item. Daily data is the most recent change detected within a calendar day for each configuration item.

Data retention settings do not affect the data for a node’s baseline configuration. Baseline information is kept forever.

By default, detailed data is kept for 7 days, hourly data is kept for 30 days, and daily data is kept for 365 days.

The default values for each level of granularity can be changed in SCM Settings:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.

2. Click the Data Retention tab.

3. Change the settings for each level of data as desired, and then click Save Changes.

**Watch for specific configuration changes in SCM**

You can now add the Recent Configuration Changes widget to any dashboard in Server Configuration Monitor (SCM).

To create the widget, go to the Server Configuration Summary page in SCM.

1. Hover over the pencil icon in the left column.

2. Click Customize page.
3. Click Page settings.

4. In Column 2, click to highlight Recent Configuration Changes.
5. In the column of icons beside Column 2, click the third icon to clone selected resources.

6. Click Done.
7. Go to the cloned instance of Recent Configuration Changes, and click Edit on the top left of the widget.
8. Select any of the pre-defined filters (Node name, Machine type, Server configuration profile, or Server configuration item) for recent configuration changes, and then click Save.

The widget displays only configuration changes that match the criteria you select. You can add more Recent Configuration Changes widgets with different filters to your dashboard.
View the structural diff in SCM

Structural diff mode has been added to the Content diff mode page in Server Configuration Monitor (SCM). If the diff engine recognizes valid JSON or XML, structural diff is used for comparison by default. Structural diff means that content of JSON or XML files is compared by its values. Spaces, element positions, and other characters are not compared. If the file is invalid, then textual diff is used instead.

![Content Comparison](image1)

![Content Comparison](image2)
Server configuration profiles in SCM

Configuration profiles in Server Configuration Monitor (SCM) are collections of elements you want to monitor. Each profile element results in one or more configuration items (for example, individual files or registry entries) being monitored. There are several out-of-the-box profiles for commonly monitored elements, or you can create custom profiles with exactly the elements you want to monitor.

SCM out-of-the-box profiles

Server Configuration Monitor (SCM) comes with several predefined configuration profiles for server inventory and commonly monitored applications. These out-of-the-box configurations are:

- HW Inventory
- SW Inventory
- IIS
- Linux Essentials
- Linux Security and Permissions
- Database profiles:
  - MS SQL Server Essentials
  - PostgreSQL Essentials
  - MySQL Essentials

HW inventory profiles in Server Configuration Monitor (SCM)

The hardware (HW) inventory profile monitors changes to the server’s hardware, including:

- Drivers
- Hard drives
- Logical drives
- Memory modules
- Network interfaces
- OutOfBand management
- Peripherals
- Processors
- Removable media
- Storage controllers
- Video card
Monitoring this profile requires that Asset Inventory be enabled on the server. To enable Asset Inventory:

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, and then click List Resources in the Node Management toolbar.

2. In the list that displays, check the box next to Asset Inventory.

3. Click Submit to save your changes.

**SW inventory profiles in Server Configuration Monitor (SCM)**

The software (SW) inventory profile monitors changes to:

- Firmware
- OS updates
- Server information
- Software installed

Monitoring this profile requires that Asset Inventory be enabled on the server. To enable Asset Inventory:

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, and then click List Resources in the Node Management toolbar.

2. In the list that displays, check the box next to Asset Inventory.

3. Click Submit to save your changes.

**IIS server configuration profiles in Server Configuration Monitor (SCM)**

The IIS profile is the predefined profile for IIS servers. It monitors the following configuration files.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%WINDIR%\Microsoft.NET**\machine.config</td>
<td>The machine.config for .NET Framework settings.</td>
</tr>
<tr>
<td>Path</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>%WINDIR%\Microsoft.NET**\web.config</td>
<td>The root web.config for .NET Framework settings.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\MBSchema.xml</td>
<td>The MetaBase schema definition used in IIS 6.0 instead of applicationHost.config.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\MetaBase.xml</td>
<td>This configuration file is used in IIS 6.0 instead of applicationHost.config.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\config\administration.config</td>
<td>This configuration file stores the settings for IIS management. These settings include the list of management modules that are installed for the IIS Manager tool, as well as configuration settings for management modules.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\config\redirection.config</td>
<td>IIS 7 and later support the management of several IIS servers from a single, centralized configuration file. This configuration file contains the settings that indicate the location where the centralized configuration files are stored.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\config\schema*.xml</td>
<td>The full schema reference for config files, including default values for all properties in every section, their valid ranges, etc.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\config\applicationHost.config</td>
<td>Parsing applicationHost.config file to search for distributed configuration via web.config files specific for a particular IIS site, application or virtual directory and located within its directory.</td>
</tr>
</tbody>
</table>

All web.config files found from parsing applicationHost.config.
Linux Essentials profiles in Server Configuration Monitor (SCM)

The Linux Essentials profile is the predefined profile for monitoring the essentials of your Linux system, including file system configuration, network settings, operating system and application software, and startup configuration.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*/etc/apt/**/</td>
<td>Monitors all of the configuration files that apt uses as its sources.</td>
</tr>
<tr>
<td>fstab /etc/</td>
<td>Monitors the fstab configuration file.</td>
</tr>
<tr>
<td>*/etc/init.d/**/</td>
<td>Monitors all of the configuration scripts used to control services.</td>
</tr>
<tr>
<td>*/etc/init/**/</td>
<td>Monitors the configuration files for the init subsystem used to start services.</td>
</tr>
<tr>
<td>inittab /etc/</td>
<td>Monitors the configuration file for the initialization system.</td>
</tr>
<tr>
<td>*/etc/modprobe.d/**/</td>
<td>Monitors all of the configuration files that are used by modprobe to manage the loading of modules during the system boot.</td>
</tr>
<tr>
<td>modules /etc/</td>
<td>Monitors the list of modules to load at boot time.</td>
</tr>
<tr>
<td>*/etc/modules-load.d/</td>
<td>Monitors the list of modules to load at boot time.</td>
</tr>
<tr>
<td>sysctl.conf /etc/</td>
<td>Monitors the configuration file that sysctl uses to change kernel parameters at runtime.</td>
</tr>
<tr>
<td>*.conf /etc/sysctl.d/</td>
<td>Monitors the configuration files that sysctl uses to change kernel parameters at runtime.</td>
</tr>
<tr>
<td>yum.conf /etc/</td>
<td>Monitors the file that yum uses for global configuration.</td>
</tr>
<tr>
<td>*/etc/yum.repos.d/</td>
<td>Monitors the files that define the extra repositories yum can use.</td>
</tr>
<tr>
<td>*/etc/yum/**/</td>
<td>Monitors the files that store extra yum configurations.</td>
</tr>
<tr>
<td>Listening Ports</td>
<td>Monitors the ports the system is listening on (excludes UDP).</td>
</tr>
<tr>
<td>Networking Items</td>
<td>Monitors for changes in your networking configuration, including the system's DNS name and aliases, network interfaces, hosts file, resolve.conf file, and the nsswitch.conf file.</td>
</tr>
<tr>
<td>Services Configuration</td>
<td>Monitors the services that are enabled on the system.</td>
</tr>
<tr>
<td>Hardware Info</td>
<td>Monitors a detailed list of system information. List includes cpu (lscpu), general hardware (lshw), PCI bus (lspci), USB (lsusb), and SCSI (lsscsi).</td>
</tr>
<tr>
<td>Package List</td>
<td>Monitors all installed packages for changes (both rpm and dpkg).</td>
</tr>
<tr>
<td>Path</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Kernel Uname</td>
<td>Monitors the system's nodename, kernel-version, and kernel-release.</td>
</tr>
<tr>
<td>Block Device List</td>
<td>Monitors changes to file system block devices (via lsblk).</td>
</tr>
<tr>
<td>Mounted Filesystems</td>
<td>Monitors changes to file system mounts.</td>
</tr>
</tbody>
</table>

**Linux Security and Permission profiles in SCM**

The Linux Security and Permissions profile in Server Configuration Monitor (SCM) is the predefined profile for monitoring security, groups, and user permissions.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group /etc/</td>
<td>Monitors the group configuration file, which defines the groups to which users belong.</td>
</tr>
<tr>
<td>login.defs /etc/</td>
<td>Monitors configurations that are used as defaults by user and group utilities.</td>
</tr>
<tr>
<td>pam.conf /etc/</td>
<td>Monitors the configuration file used by PAM to define user access to server resources and applications.</td>
</tr>
<tr>
<td>*/etc/pam.d/</td>
<td>Monitors the configuration files used by PAM to define user access to server resources and applications.</td>
</tr>
<tr>
<td>passwd /etc/</td>
<td>Monitors the file that contains the attributes of all users or accounts on the system.</td>
</tr>
<tr>
<td>*.conf /etc/security/**/</td>
<td>Monitors the configuration files that control the resources available to user processes. Often used by PAM modules.</td>
</tr>
<tr>
<td>*/etc/selinux</td>
<td>Monitors the configuration files that control the behavior of Security Enhanced Linux.</td>
</tr>
<tr>
<td>World Writable Files</td>
<td>List of files that are world writable.</td>
</tr>
</tbody>
</table>

**Database profiles in SCM**

Server Configuration Monitor (SCM) offers a number of out-of-the-box database profiles. See the table below for compatible versions and a comparison of the information you can track in each database profile type:
<table>
<thead>
<tr>
<th>MS SQL Server Essentials</th>
<th>PostgreSQL Essentials</th>
<th>MySQL Essentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions of database software that are compatible with SCM out-of-the-box profiles</td>
<td>MS SQL 2012 and later</td>
<td>PostgreSQL 12.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PostgreSQL 11.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PostgreSQL 10.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PostgreSQL 9.6.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PostgreSQL 9.5.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PostgreSQL 9.4.25</td>
</tr>
<tr>
<td>Global</td>
<td>Configuration registry entries</td>
<td>Server settings</td>
</tr>
<tr>
<td></td>
<td>Query optimizer hotfixes</td>
<td>Time zones</td>
</tr>
<tr>
<td></td>
<td>Instant file initialization</td>
<td>Collations</td>
</tr>
<tr>
<td></td>
<td>Server configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSIS packages</td>
<td></td>
</tr>
<tr>
<td>Server configuration</td>
<td>Linked servers</td>
<td>Publications</td>
</tr>
<tr>
<td></td>
<td>Database files</td>
<td>Configuration files</td>
</tr>
<tr>
<td></td>
<td>Database mail</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Database options</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default data and log location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TempDB</td>
<td></td>
</tr>
<tr>
<td>DB Schema</td>
<td>MS SQL Server Essentials</td>
<td>PostgreSQL Essentials</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>Filegroups</td>
<td>Databases</td>
</tr>
<tr>
<td></td>
<td>Tables</td>
<td>Tablespaces</td>
</tr>
<tr>
<td></td>
<td>Columns</td>
<td>Tables</td>
</tr>
<tr>
<td></td>
<td>Views</td>
<td>Views</td>
</tr>
<tr>
<td></td>
<td>Indexes</td>
<td>Attributes (Columns)</td>
</tr>
<tr>
<td></td>
<td>Triggers</td>
<td>Indexes</td>
</tr>
<tr>
<td></td>
<td>Stored procedures</td>
<td>Procedures and</td>
</tr>
<tr>
<td></td>
<td>System database objects</td>
<td>functions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Users and privileges</th>
<th>MS SQL Server Essentials</th>
<th>PostgreSQL Essentials</th>
<th>MySQL Essentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Logins</td>
<td>Database roles</td>
<td>Administrable</td>
</tr>
<tr>
<td></td>
<td>Permissions</td>
<td>Authentication rules</td>
<td>role authorization</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>Users</td>
<td>Enabled roles</td>
</tr>
<tr>
<td></td>
<td>Suspect pages</td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(schema)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Table privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Column privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Role table</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>grants</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Role column</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>grants</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Role routine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>grants</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Events and jobs</th>
<th>MS SQL Server Essentials</th>
<th>PostgreSQL Essentials</th>
<th>MySQL Essentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SQL agent jobs</td>
<td>Events</td>
<td>Events</td>
</tr>
</tbody>
</table>
### Customize out-of-the-box profiles in Server Configuration Monitor (SCM)

Out-of-the-box profiles cannot be edited directly. However, you can create a custom profile based on one of the out-of-the-box profiles, which can be edited.

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.

2. Click the Manage Profiles tab, if it is not selected by default.

3. Select the profile you wish to copy, then click Copy. An Add configuration profile window opens.

4. Make the desired changes to the list of configuration elements, description, and profile name.

5. Click Add to save the new profile.

### Profile element types in SCM

**File**

The File element type in Server Configuration Monitor (SCM) is defined by a full path to a Linux file (applicable to Linux nodes only) or to a Windows node only (applicable to Windows nodes only). This path can use the wild character * for any part of the filename, the wild character ** for any subdirectory, and system variables. File elements do not require credentials, but you can use credentials with them. To add credentials, see [Specify element credentials](#).

**Example of File type using Linux:**

- /etc/updatedb.conf
- $MODULESHOME/*.xml

**Example of File type using Windows:**
The use of wild characters can have a negative impact on performance if used to monitor too many files, or very large files.

Important to note:

- File elements using Linux are polled every minute.
- File elements using Windows are polled in near real time. However, if the FIM driver is disabled, they are polled every minute.
- Assigning an incompatible file to a node (such as a Linux file to a Windows node) will result in an error.
- Linux file elements are set to ignore symbolic links.

Windows Registry

Registry elements are defined by a registry key path. No wild characters are allowed. All subtrees are monitored, which might affect performance if monitoring a large registry tree.

For example:

- HKEY_CLASSES_ROOT\Installer\Features
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate

Windows registry elements are polled in near real time. However, if the FIM driver is disabled, they are polled every minute. Registry elements do not require credentials, but you can use credentials with them. To add credentials, see Specify element credentials.

Parsed File

This element type is only available as part of out-of-the-box profiles.

A file parser reads a particular type of file and finds more configuration elements to monitor based on that file’s contents.

<table>
<thead>
<tr>
<th>Parser</th>
<th>File parsed</th>
<th>Elements Parsed Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS Web Config Parser</td>
<td>applicationHost.config</td>
<td>This parser reads an applicationHost.config file to find web.config files to monitor for all IIS sites, applications, and virtual directories within that applicationHost.config.</td>
</tr>
</tbody>
</table>
**Internal Query**

This element type is only available as part of [out-of-the-box profiles](#).

Internal Query elements are queries to the Orion database.

**PowerShell Script**

You can create an SCM profile with the PowerShell script element and assign it to desired nodes. SCM collects the output of your custom PowerShell scripts and alerts you when it changes so that you can compare data outputs over time. PowerShell elements are polled every five minutes by default, but this interval frequency can be adjusted in settings. See [Take advantage of PowerShell script support](#) to learn more about using PowerShell in SCM.

Created by Microsoft, PowerShell is a task automation and configuration management framework that consists of a command-line shell and associated scripting language, built on the .NET Framework. PowerShell script elements do not require credentials, but you can use credentials with them. To add credentials, see [Specify element credentials](#).

![SolarWinds recommends that you avoid using credentials or other sensitive information in PowerShell or Linux script content, as this information may be viewable by non-administrator SCM users.](#)

**Linux Script**

You can also create an SCM profile with the Linux script element and assign it to nodes. As with PowerShell scripts, SCM collects the output of your Linux scripts and alerts you when that output changes. You can adjust interval frequency settings if you want Linux elements to be polled more or less frequently than the default of every five minutes. See [Leverage Linux scripts in SCM](#) for more information about using Linux scripts in SCM. Linux script elements do not require credentials, but you can use credentials with them. To add credentials, see [Specify element credentials](#).

![SolarWinds recommends that you avoid using credentials or other sensitive information in PowerShell or Linux script content, as this information may be viewable by non-administrator SCM users.](#)

**Database Query**

SCM enables you to monitor changes to databases by running SQL queries to relational databases such as SQL Server, PostgreSQL, Oracle, and MySQL. To monitor databases, you must [specify element credentials](#). Windows authentication is not supported. SCM collects data through your SQL queries and then alerts you to changes to that data. See [Monitor databases for changes using SCM](#) for further details.
Specify element credentials in SCM

Server Configuration Monitor (SCM) elements, including SQL queries, scripts, registries, and files, can now be executed using custom credentials. Credentials can be added to both custom and out-of-the-box profiles (although out-of-the-box profiles cannot be edited otherwise). When creating or editing an element, you can decide what credentials can be used during polling. SCM defaults to *Use Orion default credentials* if you don’t specify credentials. This default also applies to elements that were created in previous versions of SCM. This setting means that everything is polled exactly the same as before using LOCAL_SYSTEM user on the Windows Agent and swiagent user on the Linux Agent. However, some elements, such as Database elements, require credentials, as Windows Authentication is not supported.

Adding credentials can be useful in a variety of situations. For instance, if you’re searching for a particular configuration file, and previously, the agent did not have the permissions needed to access those files, you can now change the credentials so that you can access the files you’re looking for. Similarly, if there is a PowerShell script you are trying to run, and previously, it did not have adequate permissions, you can now add credentials to that and run the script as desired.

There are a few limitations to custom credentials you should be aware of:

- Only username-password credentials are supported.
- Username length is limited to 255 characters.
- Passwords cannot be empty.

To specify credentials for a newly created element:

1. Add a configuration element for monitoring.
Add configuration element

Element type
File

Path
C:\Users\*

Path to a file. Can use the wildcard character * to match part of a file name, ** to match any subdirectory, and Windows system variables such as %WINDIR% or Linux system variables such as $HOME). Learn more

Download content

If a file is very large, you may want to disable content downloading. Downloaded content is used for line-by-line content comparison. Without it, you will still be notified of a change, but won't be able to see the line-by-line comparison.

Description
Optional

Access authentication

Configuration element may not be able to poll necessary information without proper access rights for specific server or database etc. Add necessary credentials if needed.

Use Onion default credentials

ADD TEST CANCEL
2. Under Access Authentication, select Add new credentials from the drop-down menu.

3. Enter the desired credentials, and click Add.

To set credentials for elements that have already been assigned:
1. From Server Configuration Monitor Settings, click the Assigned Elements tab, and select the elements for which you'd like to set credentials.
2. Click Set Credentials.
3. Select Connection string and Credentials for each element type (as applicable), and then click Set.

A list of all credentials that are currently in use as well as inactive credentials in your instance of SCM is available when you click the Credentials tab. From here, you may edit or delete credentials, but you can add them only using the process described above.
SCM also makes it possible to add or edit multiple elements of a specific profile at the same time. This allows you to change a credential directly rather than changing each affected element for routine password updates if you make them every 90 days. It also enables you to make a mass change on a profile to a different set of credentials. When you make this change, it updates all elements on the profile to the new credential at once. To add or edit multiple elements at the same time:

1. From the Edit configuration profile screen, select multiple configuration elements, and click Edit.
2. Select Access authentication, and use the drop-down menu to specify credentials for all selected elements. Then click Save.

Custom profiles in SCM

These tasks are not available to all Server Configuration Monitor (SCM) users. See User restrictions for details.

You can use custom profiles to create sets of files and directories you want to monitor that aren’t covered by the out-of-the-box profiles.

- Add a custom profile
- Copy an existing profile
- Edit a custom profile
- Delete a custom profile
- Enable or disable content downloading for an element
If a custom profile contains an element that targets the same file or registry as another profile, that file or registry will be reported twice. For example, if one profile is monitoring C:\foo\*.config and another is monitoring the more specific path C:\foo\bar.config, then the file C:\foo\bar.config will be doubled in SCM.

**Add a custom profile in SCM**

To add a new custom profile to Server Configuration Monitor (SCM):

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click Add at the top of the list of profiles.
3. Enter a name for the profile and (optionally) a description.
4. Add configuration elements to the profile with the Add button in the configuration elements pane.
   a. Select an element type from the drop-down menu.
   b. Enter a path or registry key for the element. See [Element types](#) for more information on permitted characters.
   c. Optional: Define a display alias for this element. If an alias is given, the element will be referred to by the alias instead of the filename or registry key.
   d. Optional: Enter a description of the element.
5. Click Add at the bottom of the dialog to save the profile.

**Copy an existing profile in SCM**

To copy an existing configuration profile in Server Configuration Monitor (SCM):

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile you wish to copy, then click Copy. An Add configuration profile window will open.
4. Click Add to save the new profile.
Edit a custom profile in SCM

To edit a custom configuration profile in Server Configuration Monitor (SCM):

1. Navigate to the Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile you wish to copy, then click Edit.
4. In the Edit configuration profile window that opens, make your desired changes. Note that the type and path of an element can't be edited in profiles that are already assigned to a node. If you need to change the type or path, add a new element with the desired properties and remove the old one.
5. Click Save to save your changes.

Delete a custom profile in SCM

Deleting a custom profile from Server Configuration Monitor (SCM) removes all polled data gathered by that profile, for all nodes. To delete a custom configuration profile:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile(s) you want to delete, and then click Delete on the menu bar.
4. A window will open informing you of any nodes the selected profile(s) are currently assigned to. Even with SCM Admin rights, you may not be able to see all the nodes a profile is assigned to due to user limitations. Ensure that the number of nodes the confirmation dialog shows is equal to the number of nodes you believe to be assigned to the profile. If you are sure you want to delete the profile(s), click Delete to confirm.

Enable or disable content downloading for an element in SCM

Server Configuration Monitor (SCM) downloads the content of configuration elements for content comparison. For very large files or very large registry keys, you may want to disable downloading to save database space and prevent performance or network traffic issues. When content downloading is disabled, changes will still be detected and reported as usual, but line-by-line content comparison will be disabled for the element.

To toggle content downloading:
1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.

2. Click the Manage Profiles tab, if it is not selected by default.

3. Select the profile that contains the element, and then click Edit.

4. Select the element for which you want to change the content downloading setting, and then click Edit.

5. Change the Download Content switch to the desired state, and then click Save.

If content downloading was enabled for an element but is later disabled, the previously downloaded content will still be kept according to the data retention settings.

Import and export profiles in SCM

Profiles can be imported and exported to facilitate collaboration with other Server Configuration Monitor (SCM) users. SCM profile files have the extension ".scm-profile". The direct editing of .scm-profile files is not recommended.

Import

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.

2. In the Manage Profiles tab, click Import.

3. Find the .scm-profile file you want to import, and then click Open.

If a profile with the same name already exists, you will be asked if you would like to import the profile as a copy.

Export

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.

2. In the Manage Profiles tab, select the profile you want to export.

3. Click Export.
Automate SCM profile import or export

This topic explains how to automate Server Configuration Monitor (SCM) profile import or export using PowerShell script.

- To create and manage SCM profiles programmatically, use create/update/delete operations on Orion.SCM.Profiles and Orion.SCM.ProfileElements entities.

- To automate the exporting or import of profiles, use ExportProfile or ImportProfile verbs on Orion.SCM.Profile entities.

- To assign profiles to nodes or unassign profiles from nodes, use AssignToNode and UnassignFromNode verbs on Orion.SCM.Profiles entities.

See the following script for an example of how to automate operations in SCM:

```
# This sample script demonstrates the use of verbs and CRUD operations provided for manipulating
# with profiles and elements. The verbs are defined by "Orion.SCM.Profiles" entity type.
#
# The script progresses in several steps, it:
# 1. Creating new profile
# 2. Add several elements
# 3. Export profile
# 4. Delete element from profile
# 5. Assign profile to node to start monitoring
# 6. Unassign profile from node
# 7. Delete profile
# 8. Import profile
# 9. Delete imported profile

# Please update the hostname and credential setup to match your configuration.
if (!(Get-PSSnapin | where {$_ .Name -eq "SwisSnapin"})) {
    Add-PSSnapin "SwisSnapin"
}

# Connect to SWIS
Write-Host "Enter Orion host name or IP address:"
$hostname = Read-Host
Write-Host "Enter Orion username:"
$username = Read-Host
Write-Host "Enter Orion password:"
$password = Read-Host -AsSecureString
$swis = Connect-Swis -host $hostname -cred $cred

#
# CREATE PROFILE
#
# Create empty profile and add few elements.
#
$profileProperties = @{
    Name = "MyNewProfile";
    Description = "This is description of my new profile";
}
$profileUri = New-SwisObject $swis -EntityType "Orion.SCM.Profiles" -Properties $profileProperties
$profile = Get-SwisObject $swis -Uri $profileUri
$profileId = $profile.ProfileID

Write-Host "New profile with ID = $profileId was created."

#
# ADD ELEMENT TO PROFILE
#
# Create new File and Registry element and assign it to created profile.
#
$elementProperties = @{
    ProfileID = $profileId;
    Type = "File";
    Description = "Monitoring XML files in Windows Logs folder.";
    Settings = @{
        Path = "%windir%\Logs\**\*xml";
        CollectContent = $true;
    };
}
$fileElementUri = New-SwisObject $swis -EntityType "Orion.SCM.ProfileElements" -Properties $elementProperties

$elementProperties = @{
    ProfileID = $profileId;
    Type = "Registry";
    Description = "Monitoring of Windows Update registry.";
    Settings = @{
        Path = "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate";
        CollectContent = $true;
    }
}

$registryElementUri = New-SwisObject $swis -EntityType "Orion.SCM.ProfileElements" -Properties $elementProperties

# EXPORT PROFILE
# Export profile and save it to file
#

$exportedProfilePath = "c:\temp\exported.scm-profile"
(Invoke-SwisVerb $swis "Orion.SCM.Profiles" "ExportProfile" @($profileId)).InnerText | Out-File -FilePath $exportedProfilePath
Write-Host "Profile was exported to $exportedProfilePath"

# This sample script demonstrates the use of verbs and CRUD operations provided for manipulating with profiles and elements. The verbs are defined by "Orion.SCM.Profiles" entity type.
#
# The script progresses in several steps, it:
# 1. Creating new profile
# 2. Add several elements
# 3. Export profile
# 4. Delete element from profile
# 5. Assign profile to node to start monitoring
# 6. Unassign profile from node
# 7. Delete profile
# 8. Import profile
# 9. Delete imported profile

# Please update the hostname and credential setup to match your configuration.
if (! (Get-PSSnapin | where {$_.Name -eq "SwisSnapin"})) {
    Add-PSSnapin "SwisSnapin"
}

# Connect to SWIS
Write-Host "Enter Orion host name or IP address:"
$hostname = Read-Host
Write-Host "Enter Orion username:"
$username = Read-Host
Write-Host "Enter Orion password:"
$password = Read-Host -AsSecureString
$swis = Connect-Swis -host $hostname -cred $cred

# CREATE PROFILE
# Create empty profile and add few elements.
#

$profileProperties = @{
    Name = "MyNewProfile";
    Description = "This is description of my new profile"
}
$profileUri = New-SwisObject $swis -EntityType "Orion.SCM.Profiles" -Properties $profileProperties
$profile = Get-SwisObject $swis -Uri $profileUri
$profileId = $profile.ProfileID

Write-Host "New profile with ID = $profileId was created."
ADD ELEMENT TO PROFILE

Create new File and Registry element and assign it to created profile.

$elementProperties = @{
    ProfileID = $profileId;
    Type = "File";
    Description = "Monitoring XML files in Windows Logs folder.";
    Settings = @{
        Path = "%windir%\Logs\**\*xml";
        CollectContent = $true;
    }
}
$fileElementUri = New-SwisObject $swis -EntityType "Orion.SCM.ProfileElements" -Properties $elementProperties

$elementProperties = @{
    ProfileID = $profileId;
    Type = "Registry";
    Description = "Monitoring of Windows Update registry.";
    Settings = @{
        Path = "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate";
        CollectContent = $true;
    }
}
$registryElementUri = New-SwisObject $swis -EntityType "Orion.SCM.ProfileElements" -Properties $elementProperties

EXPORT PROFILE

Export profile and save it to file

$exportedProfilePath = "c:\temp\exported.scm-profile"
(Invoke-SwisVerb $swis "Orion.SCM.Profiles" "ExportProfile" @ ($profileId)).InnerText | Out-File -FilePath $exportedProfilePath
Write-Host "Profile was exported to $exportedProfilePath"

#
# ASSIGN PROFILE TO NODE
#
# Select node ID and assign created profile to it.
#
# Select the node
$ip = '10.140.127.223'
$ nodeId = Get-SwisData $swis "SELECT NodeID FROM Orion.Nodes WHERE IP_Address=@ip" @{ip=$ip}
if (!$nodeId) {
    Write-Host "Can't find node with IP '$ip'."
    exit 1
}

Write-Host "Assigning new profile to node ID = $nodeId."

Invoke-SwisVerb $swis "Orion.SCM.Profiles" "AssignToNode" @(
    # Profile ID
    $profileId,
    # Node ID
    $nodeId
)

Write-Host "Profile is assigned to node and it will start monitoring entities soon. Press ENTER to continue..."

Read-Host

#
# ADD NEW ELEMENT TO PROFILE
#
# Add new element to created profile and call PollNow to immediately apply changes.
#
Write-Host "Adding new PowerShell element to profile."

$elementProperties = @{
    ProfileID = $profileID;
}
Type = "PowerShell";
DisplayAlias = "Windows Services";
Description = "Monitoring of services with their start type.";
Settings = @{
    Path = "Get-Service | Format-Table -Property ServiceName, DisplayName, StartType";
    PollingFrequency = "0:10:00";
    PollingTimeout = "0:01:00";
}
$powerShellElementUri = New-SwisObject $swis -EntityType "Orion.SCM.ProfileElements" -Properties $elementProperties
Invoke-SwisVerb $swis "Orion.SCM.ServerConfiguration" "PollNow" @( # Node ID list
    $nodeIds
) | Out-Null
Write-Host "Profile updated, configuration sent to node and it will start monitoring new PowerShell script soon. Press ENTER to clean up..."
Read-Host

#
# UNASSIGN PROFILE FROM NODE
#
# Unassign new profile from node and delete all historical data.
#
Invoke-SwisVerb $swis "Orion.SCM.Profiles" "UnassignFromNode" @( # Profile ID
    $profileId,
    # Node ID
    $nodeId,
    # Keep history data
    $false
)
Write-Host "Profile was unassigned from node ID = $nodeId."

# # DELETE ELEMENT
# # Delete element from profile.
#
Remove-SwisObject $swis -Uri $fileElementUri
Write-Host "File element was removed from new profiles."

# # DELETE PROFILE
# # Delete profile.
#
Remove-SwisObject $swis -Uri $profileUri
Write-Host "New profile was removed from database. Press ENTER to continue..."
Read-Host

# # IMPORT PROFILE
# # Import profile
#
$fileContent = Get-Content -Path $exportedProfilePath
$importedProfileId = (Invoke-SwisVerb $swis "Orion.SCM.Profiles" "ImportProfile" @($fileContent)).InnerText
Write-Host "Profile was imported with ID = $importedProfileId. Press ENTER to continue..."
Read-Host

$importedProfileUri = Get-SwisData $swis "SELECT Uri FROM Orion.SCM.Profiles WHERE ProfileID=@id" @{id=$importedProfileId}
Remove-SwisObject $swis -Uri $importedProfileUri
Write-Host "Imported profile was removed from database."
Remove-Item -Path $exportedProfilePath
Write-Host "Deleted file $exportedProfilePath"
Compare configurations over time in Server Configuration Monitor (SCM)

You can use SCM to see which configuration items changed between any two points in time, and drill down even further to see line by line what changes were made.

See configuration changes between two points in time using SCM

Server Configuration Monitor (SCM) lets you see the difference between versions of a server’s configuration. You can see which configuration elements were added, deleted, or modified and how file attributes have changed. If content downloading is enabled for a particular element, you can also see which lines of that element were added, deleted, or modified.

See which configuration elements changed

To see which configuration elements were changed between two points in time:

1. From the Node Details page of the server you would like to monitor, navigate to the Server Configuration view in the left sidebar.
2. In the Configuration Management widget, click Compare Configuration.
3. In Configuration Comparison, you are presented with two side-by-side panels that show the monitored configuration items for that node, organized by profile and element type. By default, this comparison is between the current configuration and the baseline. If no baseline is set, the comparison is instead between the current configuration and 24 hours prior.
   a. To change the date and time displayed, click the datetime on either side and select a new date and time. If a baseline is set, you can select it quickly from the datetime selection pop-up.
4. Below the configuration item comparison panels (if there are configuration item changes), you can view changes to file attributes such as permissions.

See line-by-line changes

1. Follow the steps above, or find the Configuration Details widget on the Server Configuration view of the Node Details page.
2. Click the item you want to examine the contents of.
The Content Comparison page that opens shows a line comparison of the element’s contents at the times specified on the previous page. Unchanged lines will be collapsed by default, but can be expanded by clicking on the number of unchanged lines.

Use color-coding

There are two color-coding modes for the change comparison pages: simplified, and change-type-based. With simplified color-coding, all changes are highlighted in yellow. With change-type-based color-coding, additions are shown in green, deletions in red, and modifications in blue.

To switch color-coding modes, click the three dots in the upper right of either comparison page.

Set character encoding

By default, all items in the line-by-line comparison are displayed using UTF-8 encoding. Changing the encoding changes only the way the item is displayed and does not alter the underlying data. In environments that contain other character types, such as Japanese or Traditional Chinese, users can select the appropriate encoding settings so that characters are displayed correctly when viewing content comparisons.

To select encoding settings from the SCM home screen, under Recent Configuration Changes, click on a node to view Node Details. Next, click Configuration Comparison, and then click the three dots at the upper right of the page. Select Show encoding settings.
Next, select the appropriate character encoding type from the drop-down list and click Save.

Changing the encoding for one item changes the encoding for all other configuration items created by the same profile element. For example, if you have a File element in a profile that uses a wildcard character to match all the files in a certain directory, changing the encoding for one of those files changes the encoding for all the files in the directory.

**View multiple versions of comparison content**

SCM displays a list of each unique copy of the content over time. It handles aggregation of versions, so the tracked changes roll up, and the most recent content is shown. SCM saves the number of changes that are made in that time period, and it allows you to drill down to previous versions.
To select a version from the version picker on the Content Comparison page, click the hyperlinked date above the comparison panels. You can select any of the versions listed to view it.

If aggregation occurred, you can see it in this version picker drop-down menu. The number of aggregations are listed to the right of the version time information.

**Download or copy comparison content**

You can now download or copy comparison content to the clipboard. Click the three dots on the top right side of the Comparison page, and select Copy to clipboard or Download file from the drop-down menu.

> The copy comparison content feature is available on Chromium-based browsers only.
Learn about baselines in SCM

In Server Configuration Monitor (SCM), each node can have a snapshot of all configuration items from all profiles at a particular date set as its baseline configuration. A baseline is the ideal or standard configuration for that node. It is the configuration against which you want to judge that node going forward.

After you've set a baseline, you can be alerted when a node's configuration deviates from the baseline. For example, if a node is supposed to have only a particular set of software installed, you might assign the SW Inventory profile and set the baseline to a time immediately after all the software has been installed, then turn on the Server configuration differs from baseline alert. If software is removed or additional software is installed, the alert is triggered and notifies you that something has changed.

Define or redefine a baseline individually or in bulk

Baselines can be set from the Compare Configurations page, or from the Configuration Details widget on the SCM subview of a Node Details page.

- When comparing two configurations, if you would like to set one of them as the baseline, click the three dots to the right of the datetime and choose Set as baseline.
- From Node Details, if you would like to set the current configuration as the baseline, click Set as baseline in the upper right of the Configuration Details widget.

If a profile is assigned to a node after the baseline is defined, those configuration items are not included in the baseline.

After a baseline is set on a node, it can be reset or redefined if desired. You can also set or reset baselines for multiple nodes or all nodes at once. This capability saves time and reduces the number of adjustments you need to make in SCM. This feature can facilitate the roll-out of SCM across a large environment or help you to make need bulk changes as needed.

To redefine or delete all baselines at once:

1. Go to Settings > All Settings.
2. Under Product Specific Settings, click Server Configuration Monitor Settings.
3. Click the Monitored Nodes tab.
4. Select the desired profiles and then click Redefine Baselines or Delete Baselines as applicable.
Correlate configuration changes to performance metrics in SCM

In Server Configuration Monitor (SCM), you can see how a change in server configurations may have affected the server’s performance by viewing changes on a timeline with performance metrics using the Performance Analysis Dashboard (PerfStack™).

1. Navigate to the Node Details Summary page for the node you want to examine.

2. In the Management widget, click Performance Analyzer.

Configuration changes will be shown at the bottom in blue. The X-axis shows time, and the Y-axis of the SCM portion shows how many changes were made. To view configuration change details, hover over a column of changes and click the Inspect selection in the data explorer icon. Change details are displayed in the Data Explorer to the left.
You can also manually add Server Configuration Changes to any custom PerfStack view.

1. Select a node in the Metrics Palette.
2. Find Server Configuration Changes under Status, Events, Alerts.
3. Drag and drop Server Configuration Changes into the PerfStack view.
Azure SQL database support in SCM

You can create an Azure SQL database repository database in Server Configuration Monitor (SCM). Learn more.

To migrate an existing database to Azure SQL, take the following steps:

1. Upgrade all Orion Platform products to the most version 2019.4 or later.
2. Migrate the database.
3. Run the configuration wizard and switch the database to Azure SQL.

Alert on SCM data

Alerts can be enabled or disabled and configured through the Alert Manager, found under Alerts & Activity > Alerts > Manage Alerts.

Server Configuration Monitor (SCM) comes with the following out-of-the-box alerts:

<table>
<thead>
<tr>
<th>Alert name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server configuration has changed</td>
<td>Triggers the first time any of the server configuration items being watched are changed. To reduce noise if many changes happen at once, subsequent alerts are suppressed until the alert is cleared.</td>
</tr>
<tr>
<td>Server configuration differs from baseline</td>
<td>Triggers the first time a configuration item changes in a way that does not match that server’s baseline configuration, where previously the configuration did match the baseline.</td>
</tr>
</tbody>
</table>

You can also create custom alerts using Server Configuration object fields and events, including the baseline status and when the last change was detected, as trigger conditions.
Events in Server Configuration Monitor (SCM)

You can view events in the Orion Web Console Message Center, found under Alerts & Activity, and in several widgets throughout the Orion Web Console. Server Configuration Monitor (SCM) fires the following events:

<table>
<thead>
<tr>
<th>Event text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server configuration baseline set to &lt;datetime&gt; on node '&lt;node&gt;'</td>
<td>The baseline has been set for the first time on a node.</td>
</tr>
<tr>
<td>Server configuration baseline reset to &lt;datetime&gt; on node '&lt;node&gt;'</td>
<td>The baseline has been set to a different datetime.</td>
</tr>
<tr>
<td>Server configuration differs from baseline on node '&lt;node&gt;'</td>
<td>Server’s configuration has changed and no longer matches the baseline.</td>
</tr>
<tr>
<td>Server configuration matches the baseline on node '&lt;node&gt;'</td>
<td>Server’s configuration that didn’t match the baseline before has changed to match it.</td>
</tr>
</tbody>
</table>
Report on Server Configuration Monitor (SCM) data

SolarWinds provides predefined reports for each Orion Platform product. You can use the reports as soon as there is data to be reported on.

View a list of predefined reports by clicking Reports > All Reports in the menu bar. Use the web-based interface to customize the predefined reports or create your own reports.

SCM comes with the following out-of-the-box reports:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
</table>
| List of all configuration changes detected | All configuration changes that were detected in the past 24 hours. | • Node name  
• Node IP address  
• Profile name  
• Element type  
• Configuration item name  
• Change type  
• Change timestamp |
| List baseline mismatches | All configuration items that do not match the baseline configuration for the server, the last time a change was detected for that item, what kind of change was made, and a link to compare the item to the baseline. | • Node  
• Profile  
• Configuration item  
• Most recent change detected  
• Change type  
• Link to the change comparison page |
<table>
<thead>
<tr>
<th>Nodes with SCM profiles currently assigned</th>
<th>All nodes that have at least one SCM profile assigned, and which profiles are assigned.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Node • Assigned profile</td>
</tr>
</tbody>
</table>
Explanations of error messages in SCM

You may encounter profile errors, element errors, or server configuration errors in SCM. The tables below provide explanations for these errors to help you understand next steps.

Server configuration errors

You may encounter server configuration errors when no agent is assigned to the SCM node, when the agent status indicates a problem, when an agent plugin is not deployed or indicates a problem, when automatic detections of file/registry changes does not work, or when the operating system or FIM version is not supported. Consult the following table for an explanation of these errors and then see Troubleshoot your SCM deployment for steps you can take.

<table>
<thead>
<tr>
<th>Server Configuration error messages</th>
<th>Potential Root causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent missing</td>
<td>One or more elements assigned to an SCM node require an agent, such as a file, parsed file, registry, or PowerShell, but no agent is deployed to the SCM node.</td>
</tr>
<tr>
<td>Agent issue</td>
<td>There is an agent deployed to an SCM node, and it is needed by some of its elements, but the status of the agent is different from OK or RebootRequired. Go to Manage Agents for more details.</td>
</tr>
<tr>
<td>SCM plugin issue</td>
<td>There is an agent deployed to an SCM node, and it is needed by some of its elements, but the status of the SCM agent plugin is different from Installed or NotApplicable.</td>
</tr>
<tr>
<td>SCM plugin not responding</td>
<td>There is an agent deployed to an SCM node, and it is needed by some of its elements. The SCM agent plugin seems to be deployed, but is not responsive. Go to Manage Agents for more details, or restart the agent on the node.</td>
</tr>
<tr>
<td>SCM plugin not applicable</td>
<td>There is an agent deployed to an SCM node, and it is needed by some of its elements. However, the operating system version is too old, and the SCM agent plugin cannot be deployed. For more information on operating system requirements for SCM, see SCM system requirements.</td>
</tr>
<tr>
<td>Server Configuration error messages</td>
<td>Potential Root causes</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Asset inventory missing</td>
<td>One or more profiles is assigned to the SCM node load data from asset inventory, but asset inventory is not enabled on the SCM node. Go to List Resources to enable asset inventory.</td>
</tr>
<tr>
<td>FIM not supported version</td>
<td>One or more elements assigned to the SCM node use FIM, but the FIM version already installed on the target machine is not compatible with the current version of SCM and cannot be upgraded automatically. See also <a href="#">Troubleshoot FIM driver issues in SCM</a>.</td>
</tr>
<tr>
<td>FIM version error</td>
<td>One or more elements assigned to the SCM node use FIM, but the version of the FIM installed on the target machine cannot be detected. See also <a href="#">Troubleshoot FIM driver issues in SCM</a>.</td>
</tr>
<tr>
<td>FIM install error</td>
<td>One or more elements assigned to the SCM node use FIM, but the FIM installation on the target machine failed.</td>
</tr>
<tr>
<td>FIM load error</td>
<td>One or more elements assigned to the SCM node use FIM, but the FIM on the target machine could not be started or configured in a timely manner. See also <a href="#">Troubleshoot FIM driver issues in SCM</a>.</td>
</tr>
<tr>
<td>FIM initialization timeout</td>
<td></td>
</tr>
<tr>
<td>Server configuration polling is disabled due to insufficient license</td>
<td>A server configuration is not covered, or its parent node is not covered by a valid node license. Polling on that SCM node is stopped.</td>
</tr>
</tbody>
</table>

**Errors assigning elements to incompatible platforms**

You may encounter profile errors if you attempt to assign a profile to an incompatible node. Consult the guidelines in the following table for proper profile assignment.
<table>
<thead>
<tr>
<th>Node Type</th>
<th>Assigned Element Type</th>
<th>Compatible Assignment?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows server</td>
<td>File with Windows filepath</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>File with Linux filepath</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Registry element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Linux/UNIX script element</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>PowerShell script element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>HW/SW inventory element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SWIS (internal query) element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Parsed file element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Mixed Windows and Linux elements</td>
<td>No</td>
</tr>
<tr>
<td>Linux Server</td>
<td>File with Windows filepath</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>File with Linux filepath</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Registry element</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Linux/UNIX script element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>PowerShell script element</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>HW/SW inventory element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SWIS (internal query) element</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Parsed file element</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Mixed Windows and Linux elements</td>
<td>No</td>
</tr>
</tbody>
</table>

**Element errors**

You may encounter element errors if SCM doesn’t have sufficient permissions or if something blocks its permissions. Consult the following table for an explanation of these errors.
<table>
<thead>
<tr>
<th>Element error messages</th>
<th>Potential root causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>SCM cannot access a configuration file, a folder referenced by a configuration element, or the monitored folder.</td>
</tr>
<tr>
<td>Access denied</td>
<td></td>
</tr>
<tr>
<td>Parsed file not found</td>
<td>SCM cannot store a PowerShell query result or a SWIS query result in temporary files on an agent or poller.</td>
</tr>
<tr>
<td>Script execution timeout</td>
<td>SCM cannot read a monitored registry key on the agent or the modification time on an agent.</td>
</tr>
<tr>
<td>Script execution error</td>
<td>SCM cannot create a temporary copy of an exported registry file or a temporary copy of a monitored file on an agent.</td>
</tr>
<tr>
<td>Polling failed</td>
<td>SCM cannot move a temporary file on a poller.</td>
</tr>
<tr>
<td></td>
<td>SCM was unable to find a configuration file to be parsed (for example, applicationHost.config).</td>
</tr>
<tr>
<td></td>
<td>A PowerShell script execution failed, and error output was collected to describe the execution errors.</td>
</tr>
<tr>
<td></td>
<td>A PowerShell script or an exporting registry took too long to finish.</td>
</tr>
<tr>
<td></td>
<td>There is no connection to the database or credential, and polling failed.</td>
</tr>
</tbody>
</table>
Troubleshoot your SCM deployment

The following are steps you can take to troubleshoot issues with your Server Configuration Monitor (SCM) deployment.

- If you aren't seeing any configuration data for a node, click Poll Now on the Node Details page. SCM may take up to an hour to poll data initially, but clicking Poll Now should result in data appearing within a few minutes.

- If you’re experiencing polling issues, try troubleshooting the Orion Agent.

- If you’re experiencing polling issues with only certain configuration items, make sure the system account on the node has permissions to the monitored file/registry path.

- Ensure that the Module Engine, SWIS, Job Engine, Collector Service, Agent and Website Orion services are running on your Orion server.

If the above steps don’t resolve your issue, check the SCM logs for more information. By default, the relevant log files are located at:

- C:\ProgramData\SolarWinds\Logs\Agent\SolarWinds.Orion.SCM.AgentPlugin.log
- C:\ProgramData\Solarwinds\Collector\Logs\Collector.Service.log
- C:\ProgramData\Solarwinds\Logs\SCM\BL\BusinessLayer.log
Troubleshoot FIM driver issues in SCM

The following is a description of the cause and resolution for the issue that occurs when the FIM driver, which is required for real-time monitoring, does not work properly in Server Configuration Monitor (SCM).

Cause

The FIM driver can fail to initialize due to the following errors:

- The FIM driver is already installed, but the version is not as current as required.
- The FIM driver is already installed, but the version is not compatible.
- The installation of the FIM driver failed.
- Loading of the FIM driver failed.
- Initialization of the FIM driver timed out. (Timeout is set to 30 seconds.)
- Another exception occurred.
Steps

1. To determine whether SWFs2Fltr (the FIM driver) is correctly installed and loaded, enter the following command line:

   fltmc

2. Check to see if SWFs2Fltr is in the list:

   ![Filter List](image1)

3. If the filter is not loaded, enter the following command line:

   driverquery

4. Check to see if the SWFs2Fltr driver is in the list:

   ![Driver List](image2)

5. If the driver is not in the list, try to install it manually. Go to the SCM agent plugin folder by entering the following command:

   cd “c:\Program Files (x86)\SolarWinds\Agent\Plugins\SCM”
6. Enter the following command:

```
RUNDLL32.exe SETUPARI.DLL, InstallHinfSection DefaultInstall 128 .\SWFsFltrv2.inf
```

7. If no error message is displayed, the driver is installed, and you can check it using the driverquery command (as above).

8. Try to load the driver by entering the following command:

```
fltmc load SWFsV2Fltr
```

9. Determine whether you see output.

- If no, then loading of the filter succeeded, and you can check it using the fltmc command.

- If yes, then loading of the driver failed. For example, the following error is displayed when the driver is not installed:

```
Load failed with error: 0x80070002
The system cannot find the file specified.
```