®

SolarWinds Hybrid Cloud Observability for Federal Government Version 2024.2.1 Common Criteria Supplement

Version 1.1

October 22, 2024

SolarWinds Worldwide, LLC
7171 Southwest Parkway
Building 400
Austin, Texas 78735

DOCUMENT INTRODUCTION

Prepared By:
SolarWinds Worldwide, LLC
7171 Southwest Parkway
Building 400
Austin, Texas 78735
http://www.solarwinds.com

REVISION HISTORY

Rev	Description
1.0	July 01, 2024 – Initial release.
1.1	October 22, 2024 – Updated the TOE version to 2024.2.1.

TABLE OF CONTENTS

ACRONYMS LIST

CC	**Common Criteria**
DBMS	**DataBase Management System**
DNS	**Domain Name System**
EOC	**SolarWinds Enterprise Operations Console™**
HTTP	**HyperText Transfer Protocol**
HTTPS	**HTTP Secure**
IIS	**Microsoft Internet Information Services**
IP	**Internet Protocol**
IPAM	**SolarWinds IP Address Manager™**
IT	**Information Technology**
LAN	**Local Area Network**
LA	**SolarWinds Log Analyzer™**
NCM	**SolarWinds Network Configuration Manager™**
NPM	**SolarWinds Network Performance Monitor™**
NTA	**SolarWinds NetFlow Traffic Analyzer™**
REST	**REpresentational State Transfer**
SAM	**SolarWinds Server & Application Monitor™**
SCM	**SolarWinds Server Configuration Monitor™**
SIEM	**Security Information and Event Management**
SRM	**SolarWinds Storage Resource Monitor™**
SSL	**Secure Socket Layer**
TCP	**Transmission Control Protocol**
TFTP	**Trivial File Transfer Protocol**
TLS	**Transport Layer Security**
TOE	**Target Of Evaluation**
TSF	**TOE Security Function**
UDT	**SolarWinds User Device Tracker™**
VMAN	**SolarWinds Virtualization Manager™**
VNQM	**SolarWinds VoIP & Network Quality Manager™**
WPM	**SolarWinds Web Performance Monitor™**

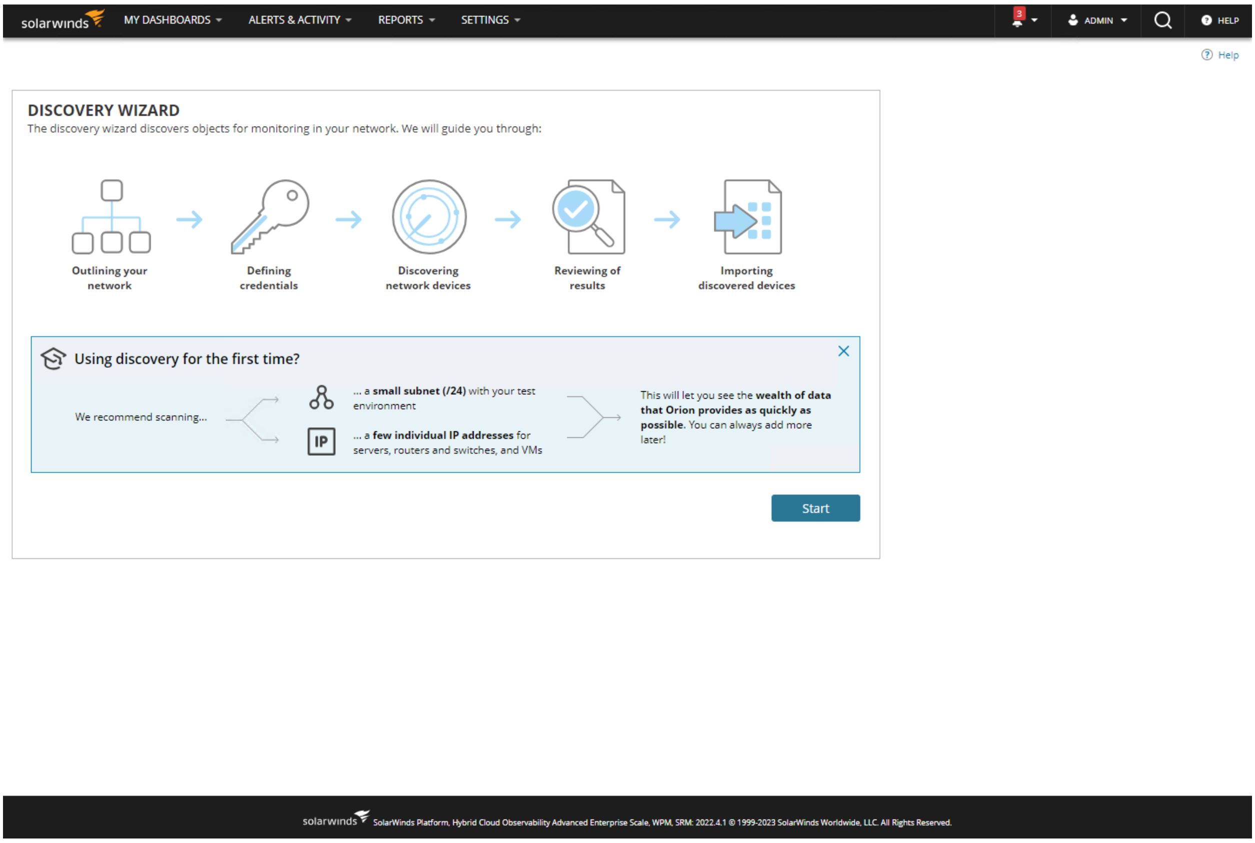
1. Introduction

This document provides guidance to customers to install and use the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 in accordance with the evaluated configuration specified for the Common Criteria evaluation.

The SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 advanced licensing option includes the following components:

- SolarWinds Platform V2024.2.1
- Enterprise Operations Console (EOC) 2024.2.1,
- IP Address Manager (IPAM) V2024.2.1,
- Log Analyzer (LA) V2024.2.1,
- Network Configuration Manager (NCM) V2024.2.1,
- Network Performance Monitor (NPM) V2024.2.1,
- NetFlow Traffic Analyzer (NTA) V2024.2.1,
- Server & Application Monitor (SAM) V2024.2.1,
- Server Configuration Monitor (SCM) V2024.2.1,
- Storage Resource Monitor (SRM) 2024.2.1,
- User Device Tracker (UDT) V2024.2.1,
- Virtualization Manager (VMAN) V2024.2.1,
- VoIP & Network Quality Manager (VNQM) V2024.2.1, and
- Web Performance Monitor (WPM) 2024.2.1

The module version numbers can be verified by viewing the bottom of the screen in the SolarWinds Web Console. The HCO Advanced licensing option consists of a single version number for all components except SRM and WPM modules and is displayed at the bottom of the SolarWinds Web Console.



DISCOVERY WIZARD

The discovery wizard discovers objects for monitoring in your network. We will guide you through:

Using discovery for the first time?

We recommend scanning...

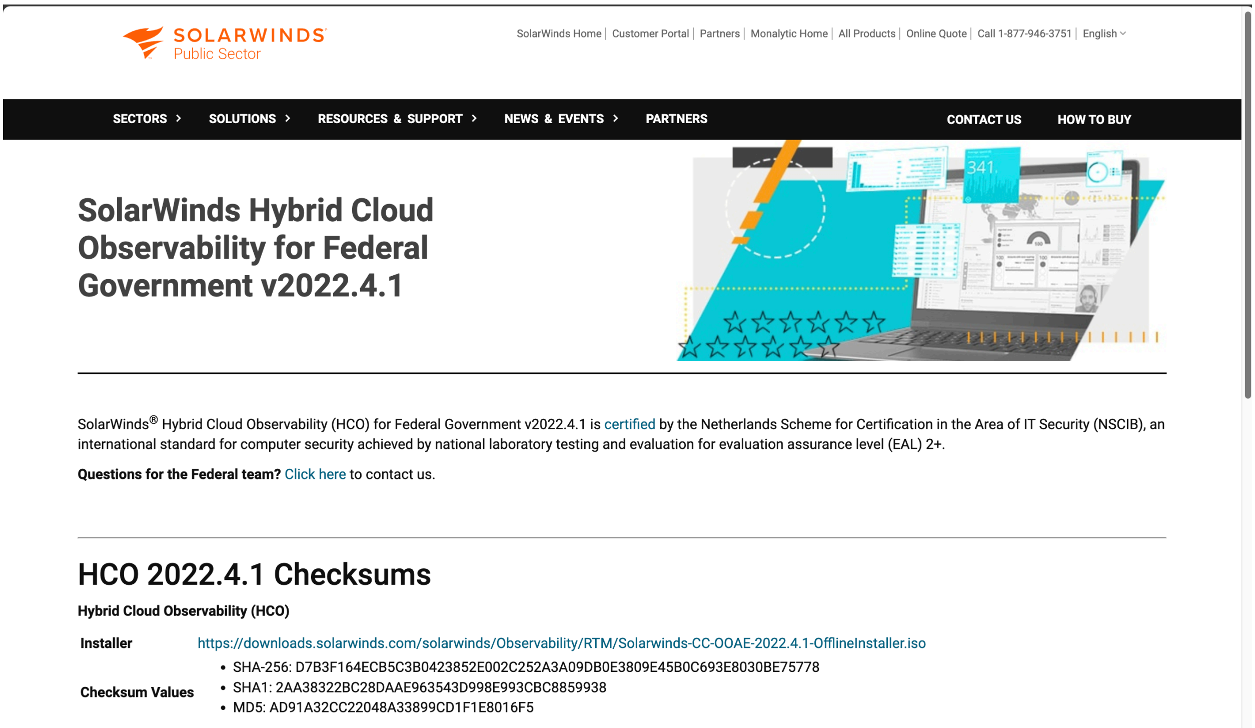
... a **small subnet (/24)** with your test environment

... a **few individual IP addresses** for servers, routers and switches, and VMs

This will let you see the **wealth of data that Orion provides as quickly as possible.** You can always add more later!

solarwinds SolarWinds Platform, Hybrid Cloud Observability Advanced Enterprise Scale, WPM, SRM: 2022.4.1 © 1999-2023 SolarWinds Worldwide, LLC. All Rights Reserved.

These are the module numbers listed on the SolarWinds Hybrid Cloud Observability for Federal Government website:


SOLARWINDS
Public Sector
SolarWinds Home | Customer Portal | Partners | Monalytic Home | All Products | Online Quote | Call 1-877-946-3751 | English
SECTORS
SOLUTIONS
RESOURCES & SUPPORT
NEWS & EVENTS
PARTNERS
CONTACT US
HOW TO BUY
341

SolarWinds Hybrid Cloud Observability for Federal Government v2022.4.1

SolarWinds® Hybrid Cloud Observability (HCO) for Federal Government v2022.4.1 is certified by the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), an international standard for computer security achieved by national laboratory testing and evaluation for evaluation assurance level (EAL) 2+.

Questions for the Federal team? Click here to contact us.

HCO 2022.4.1 Checksums

Hybrid Cloud Observability (HCO)

Installer	https://downloads.solarwinds.com/solarwinds/Observability/RTM/Solarwinds-CC-OOAE-2022.4.1-OfflineInstaller.iso
Checksum Values	• SHA-256: D7B3F164ECB5C3B0423852E002C252A3A09DB0E3809E45B0C693E8030BE75778 • SHA1: 2AA38322BC28DAAE963543D998E993CBC8859938 • MD5: AD91A32CC22048A33899CD1F1E8016F5

2. Configuration Constraints

The SolarWinds Hybrid Cloud Observability is installed on multiple Windows servers dedicated to the SolarWinds Platform function. The evaluated configuration consists of the following:

1. One instance of the EOC, installed on a single dedicated Windows server.
2. One or more instances of the SolarWinds Platform Server, each installed on a dedicated Windows server. Each SolarWinds Platform Server has NPM, SAM, NCM, NTA, IPAM, UDT, SRM, WPM, VMAN, SCM, LA, and VNQM installed.
3. For each instance of the SolarWinds Platform Server, a database (and DBMS) is installed on a separate dedicated Windows server.

In order to operate in accordance with the Common Criteria evaluated configuration, the following configuration constraints must be adhered to:

1. IIS on all the dedicated Windows servers hosting components is configured to accept HTTPS connections only.
2. Session timeouts are not disabled for user accounts, and the Session Timeout for web users is configured as a non-zero value.
3. Windows Account Login is not enabled for the Web Console.
4. Enable Audit Trails is selected.
5. Access to the Windows applications is restricted in Windows to users authorized to perform those functions, in particular: manage Alerts, and manage Report configuration settings.
6. The Customize option is not configured for any menu bars for the Web Console.
7. Custom IPAM roles are not defined; the built-in IPAM roles are used exclusively.
8. Properties of IPAM-specific entities are not used to delegate access.
9. The SAM and WPM components allow for separately-configurable roles. The evaluated configuration requires the SAM and WPM component-specific roles to be configured the same as the SolarWinds Platform role (Administrator or User).
10. The NTA Database Maintenance option is enabled in order to automatically compress and purge data according to the configured periods.
11. When importing User Accounts, only individual accounts are imported. Windows Group Accounts are not imported.
12. Only Administrators assign passwords for User Accounts. Non-Administrators are not permitted to change their own passwords.
13. The Server Browser Integration parameter is not enabled for User Accounts.
14. Reports are managed via the SolarWinds Platform Web Console rather than the Report Writer Windows application (legacy).
15. Custom Configuration Change Templates are not configured or evaluated. The default configuration change templates are included in the evaluation.
16. Real-time config change notification is not enabled in NCM since it is dependent on additional software beyond the scope of the evaluated components.
17. Per-device credentials are used rather than per-user device credentials.
18. If TFTP is used to exchange configuration files with Nodes, the TFTP service is restricted to requests from authorized Nodes.
19. The SolarWinds Engineer’s Toolset optional component is not installed.
20. External web sites are not added to SolarWinds Platform Web Console views.

21. The "Check for product updates" function is disabled. Installing product updates may update the product to a version that has not been evaluated.
22. Custom device pollers are not configured or evaluated. Pollers supplied with SolarWinds Platform are included in the evaluation.
23. Custom component monitors are not configured or evaluated. Component monitors supplied with SolarWinds Platform are included in the evaluation.
24. Custom property functionality is not configured or evaluated. Built-in properties are included in the evaluation and may be used to configure View limitations.
25. Advanced Alerts are not configured or evaluated. Basic Alerts are included in the evaluation.
26. Customized Views are not configured on SolarWinds Platform Web Consoles.
27. View Limitations are not configured.
28. Custom account limitations are not configured.
29. The functionality to remotely manage interfaces in Network Devices is not evaluated.
30. Custom NCM device templates are not configured or evaluated. The default device templates supplied with SolarWinds Platform are included in the evaluation.
31. Custom SCM configuration profiles are not configured or evaluated. The default out-of-the-box application and server configuration profiles supplied with SCM are included in the evaluation.
32. Custom LA log-processing rules are not configured or evaluated. The default out-of-the-box log-processing rules supplied with LA are included in the evaluation.
33. The Allow User To Personalize Their Pages permission is not set for any EOC user accounts. Therefore, only the default page views are included in the evaluation.
34. By default, the pre-defined Admin account has no password. A password must be configured for this account during installation.
35. SolarWinds recommends the use of SNMP v3 for communication with remote IT systems. However, depending on the protections implemented in the Operational Environment for traffic between SolarWinds Platform components and the remote IT systems, any SNMP versions may also be acceptable. This determination is made by administrators for individual environments.
36. User credential validation by an LDAP server is not configured in SolarWinds Platform; user credential validation is performed by SolarWinds Platform.
37. During installation of EOC, Windows-based authentication must be selected. Each EOC user account added to the configuration must specify Windows individual user accounts. Follow the procedures in the "Create users based on existing Active Directory or local domain accounts" section of the EOC Getting Started guide when adding EOC users.
38. The SolarWinds Report Writer application must be deleted from the SolarWinds Platform Server after installation. Alternatively, access can be restricted so no one can use the application.
39. Admins may choose to restrict access to certain information used by SWQL and SWIS. For maximum security, SolarWinds recommends setting up a firewall to restrict access and reject any connections to port 17777 other than the communication between EOC and the SolarWinds Platform Server. Admins can also limit user access by adding limitations in the Account Limitations section of Manage Accounts in the SolarWinds Platform Console.
40. To limit any potential XSS vulnerabilities, SolarWinds recommends restricting access based on roles, avoiding un-necessary access, and enforcing the strictest access

control for all users via the Manage Accounts page in the SolarWinds Platform Web Console. Admins should also confirm or configure multifactor authentication.

41. To reduce vulnerabilities, SolarWinds recommends:
    1. Setting the session timeout for Logouts to 10 minutes (the default value is 25 minutes).
    2. Applying proper segmentation controls on the network where you deploy the SolarWinds Platform and SQL Server instances.
    3. Separating your SolarWinds Platform servers from your infrastructure on managed VLANs and jumpboxes.
    4. Implementing strict access control and auditing in your environment at operating system and network layers. Limit access to the SolarWinds Platform and SQL server instances to only those authorized persons who require access as part of their duties.
42. To reduce the risk of leaking any stacktrace information, Admins can use a firewall to restrict access to SWIS REST API service only to the SolarWinds Platform and EOC servers. Admins can also remove stacktrace information from error messages displayed in the SolarWinds Platform Web Console by disabling "IncludeErrorDetails" setting in the Advanced Configuration.
43. Admins may choose to follow best security practices and disable TLS 1.0, RC4 ciphers and medium strength cipher suites like 3DES-CBC on servers hosting SolarWinds Platform and SolarWinds Enterprise Operations Console software.

The following functionality provided by SolarWinds Hybrid Cloud Observability 2024.2.1 is not evaluated:

- Create a custom poller to monitor any SNMP-enabled device, collect detailed data from MIB tables, and monitor virtually any statistic available on network devices.
- Install additional polling engines for large networks with a small number of NPM or SAM instances.
- Install additional web servers to support a large number of network managers.
- External web sites are not added to SolarWinds Platform Web Console views.
- The "Check for product updates" function is not used.
- Custom device pollers are not configured. SolarWinds Platform allows user to extend monitoring functionality by creating several types of pollers (an example how to create a new poller - https://support.solarwinds.com/SuccessCenter/s/article/Create-a-Universal-Device-Poller-UnDP). By default in clean SolarWinds Platform installation there are no custom pollers configured. SolarWinds Platform comes with a set of built-in (shipped by SolarWinds) pollers used to monitor different metrics, e.g. temperature of devices, load of CPU, memory available etc. Pollers supplied by SolarWinds are under evaluation.
- Custom component monitors are not configured. SolarWinds Platform allows user to create new component monitors to monitor their own custom application (an example how to create one component monitor - https://support.solarwinds.com/SuccessCenter/s/article/Creating-a-new-application-template-Video). By default in clean SolarWinds Platform installation there are no custom component monitors configured. Component monitors supplied by SolarWinds are under evaluation. Account limitations are tied to custom component monitors and are also not configured.
- Custom property functionality is not configured. Built-in properties are under evaluation.
- The functionality to remotely manage interfaces in Network Devices.

- Custom NCM device templates are not configured. SolarWinds Platform allows user to create new NCM device templates to monitor any specific devices or metrics (more information on NCM device template - https://documentation.solarwinds.com/en/Success_Center/NCM/Content/NCM-About-device-templates.htm). By default in a clean SolarWinds Platform installation there are no custom NCM device templates. The default device templates supplied by SolarWinds are under evaluation.
- Customized SCM custom profiles are not configured. Similar as NCM device templates, SolarWinds platform allows user to create their own SCM custom profile to monitor any specific system or metrics (more information on SCM custom profile - https://documentation.solarwinds.com/en/success_center/scm/Content/SCM-Custom-profiles.htm). The default profile supplied by SolarWinds are under evaluation.
- Customized views are not configured on SolarWinds Platform Web Consoles. SolarWinds Platform allows user to create their own customized views, such as configurable pages or network information that can include e.g. maps, charts, events, summary lists, links to other resources or reports (more information on customized views - https://documentation.solarwinds.com/en/success_center/orionplatform/Content/Core-Customizing-Views-sw1376.htm). By default in a clean SolarWinds Platform installation there are no customized views configured. The default views supplied by SolarWinds are used and under evaluation.
- View Limitations are not configured. SolarWinds Platform has a capability to limit which devices are displayed on a view (page). By default on clean installation there are no view limitations configured.
- Customized account limitations are not configured on SolarWinds Platform Web Consoles. SolarWinds Platform has capability to configure account limitations, similar to view limitations (apply to a specific view only), and it will restrict displayed devices for user on all views (pages). By default on clean installation there are no custom account limitations setup. Predefined account limitations provided by SolarWinds may be configured for evaluation.
- Customized page views are not configured on EOC Web Consoles. Similar as SolarWinds Platform, EOC allows user to create their own customized views. By default in clean EOC installation there are no customized views configured. The default views supplied by SolarWinds are used (the Allow User To Personalize Their Pages permission is not set) and under evaluation.
- Agents providing an alternative to WMI or SNMP for gathering information from monitored systems are not configured. Customers can deploy Agents (a small binary file / service provided by SolarWinds) in remote hosts to pull data. For example, if customers had firewalls setup that don't allow ingress traffic, it will be useful to install an Agent in a protected subnet and connect in an Agent-initiated way to SolarWinds Platform. Otherwise SolarWinds Platform would not be able to reach those devices. Agents installed on remote node and the connections with those Agents are excluded from evaluation. Agents installed by default on the host which runs the TOE are under evaluation.(more detail on it - https://documentation.solarwinds.com/en/success_center/orionplatform/Content/Core-Deploying-an-Agent-sw422.htm).
- Alert Limitations are not configured. Similar as other limitations (view limitation and account limitation), this functionality will limit access (view or edit) to alerts for specific user. By default such limitations are not configured.
- Alert Custom Properties are not configured. SolarWinds Platform has a concept of Custom Properties which are additional fields that can describe better monitored objects,

such as responsible team, business unit, owner in organization etc. Those fields can be created by customer via SolarWinds Platform Web Console. Such properties can also be used for Alerts to help organize them. Such custom properties for alerts should not be configured for evaluation and that’s the default for clean SolarWinds Platform installations.

- Advanced Alert Options are not configured. SolarWinds Platform provides a wizard for guiding user through process of alert creation. One of the steps is defining conditions that will trigger an alert. Advanced Alert Options make it possible to create complex conditions (https://www.solarwinds.com/documentation/en/flarehelp/orionplatform/content/core-building-complex-conditions-sw971.htm?cshid=orioncoreag_alertsbuildingcomplexconditions). This functionality should not be enabled for user specified alert for evaluation.
- Alert actions are limited to sending syslog and/or SNMP Trap messages. Other actions (e.g., sending e-mail, Dialing a Paging, or SMS Service) are excluded from the evaluation.
- Each SolarWinds Platform Server may have any combination of NPM, SAM, NCM, NTA, IPAM, UDT, LA, WPM, SCM, SRM, VMAN, and/or VNQM installed. Evaluation testing only includes scenarios with all components installed.
- NCM includes the ability to execute scripts on network devices. This functionality is excluded from the evaluation.
- NCM supports multiple protocols to request and transfer configuration files from network devices. Only SNMP to request files and TFTP to transfer files are under evaluation.
- SolarWinds recommends the use of SFTP and SCP to upload files containing security information from monitored devices. SolarWinds recommends encrypting security information (e.g., passwords in the device configuration file) transmitted to SolarWinds Platform from the monitored device if device allows that.
- Validation of web interface user credentials is performed by SolarWinds Platform. Validation by an LDAP server is not configured. SolarWinds Platform has a functionality that allows to use Windows Authentication with Active Directory for authentication (https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Core-Windows-Authentication-with-Active-Directory-sw2411.htm). It’s by default not configured, and should not be used.
- SolarWinds Platform High Availability (HA) features automatic failover to a secondary server to ensure continuous monitoring when a component failure occurs. This functionality is excluded from the evaluation.
- The REST interface is not used.
- UDT provides the ability to send commands to network devices to shut down a port. This functionality is excluded from the evaluation.

3. Requirements for the Operational Environment

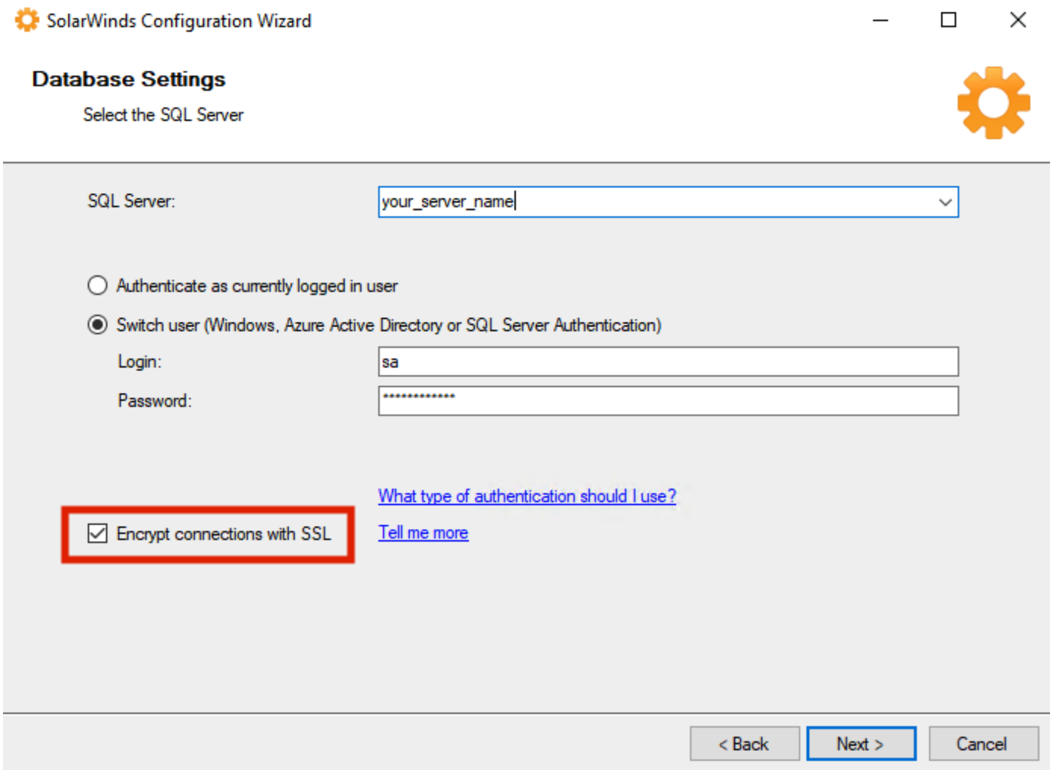
In order for SolarWinds Platform software to function securely, the operational environment supporting it and the administrators that manage it must satisfy the following requirements:

1. The Operational Environment will protect communication between the TOE and systems outside the TOE.
2. The Operational Environment will provide cryptographic functionality to protect protocol communication with remote IT systems.
3. The Operational Environment will require incoming connections to the Web Services to use SSL/TLS (HTTPS).
4. The Operational Environment will require users of the IT systems hosting the SolarWinds Platform software to successfully identify and authenticate themselves with Windows before usage of those systems is allowed.
5. Administrators must ensure that access to the SolarWinds Platform databases via Windows or the DBMS is restricted to authorized users only.
6. Administrators will monitor disk space usage of the SolarWinds Platform databases and take proactive steps to protect against data loss.
7. Administrators will install the SolarWinds Platform software in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
8. Administrators will install and configure the SolarWinds Platform software according to the administrator guidance.
9. Administrators will install and configure a network that supports communication between the distributed SolarWinds Platform components. The administrator will ensure that this network functions properly.
10. Administrators are non-hostile.
11. Administration is competent and on-going.
12. Administrators of the IT systems hosting the SolarWinds Platform software configure Windows to limit access to the applications that invoke SolarWinds Platform Server functionality to users authorized to invoke SolarWinds Platform management functionality.
13. Administrators use the Web Console only for any functions that can be performed both via the Web Consoles and via Windows applications.
14. The Operational Environment will provide reliable timestamps to SolarWinds Platform services and applications. Note: The Microsoft Windows Server Operating System synchronizes Windows servers with an NTP server. The SolarWinds Platform does not require any additional synchronization. The SolarWinds Platform products use the local server and SQL Server time settings.

Additional requirements for securing TSF Data:

1. Administrators must ensure that the Operational Environment will request encrypted DBMS connections and transmit the TSF data to/from the database with TLS encryption, by enabling “Encrypt connections with SSL” in the SolarWinds Platform Configuration Wizard. The SolarWinds Platform Configuration Wizard runs automatically the first time you install any SolarWinds Platform module. It is

suggested that a valid certificate is imported into SQL Server and used for TLS encryption, else SQL Server automatically creates a self-signed certificate for TLS communication.



SolarWinds Configuration Wizard

Database Settings

Select the SQL Server

SQL Server: your_server_name

○ Authenticate as currently logged in user

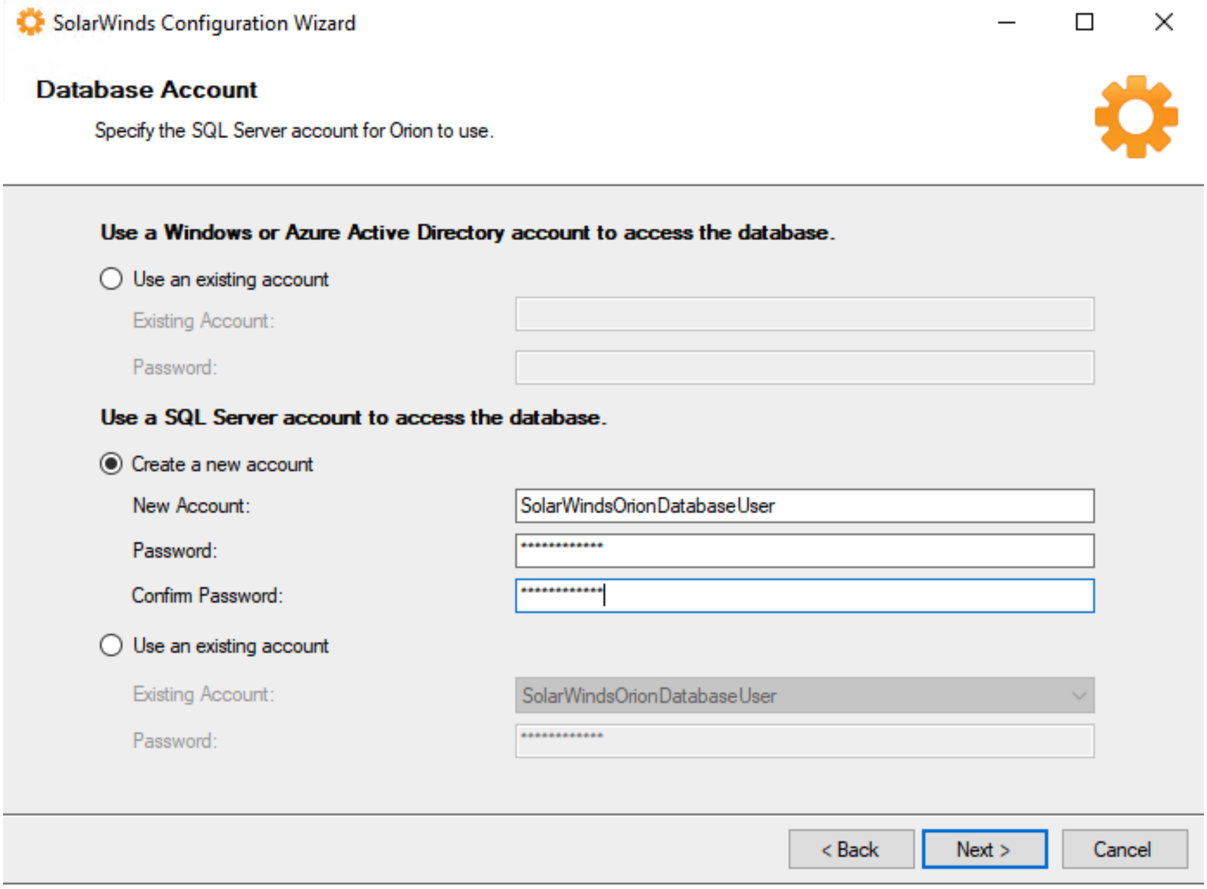
● Switch user (Windows, Azure Active Directory or SQL Server Authentication)

Login: sa

Password: ************

☑ Encrypt connections with SSL

2. To further secure and force encrypted connectivity between the DBMS and SolarWinds Platform, the “Force Encryption” option should be enabled in the Microsoft SQL Server configuration. This can be done by following these steps:
    a. Configure the server to force encrypted connections.
    b. In SQL Server Configuration Manager, expand SQL Server Network Configuration, right-click Protocols for <server instance>, and then select Properties.
    c. In the Protocols for <instance name> Properties dialog box, on the Certificate tab, select the desired certificate from the drop-down for the Certificate box, and then click OK.
    d. On the Flags tab, in the ForceEncryption box, select Yes, and then click OK to close the dialog box.
    e. Restart the SQL Server service.
3. Administrators must use best practices around granting access with least privileges, and ensure that a different account, other than the Super Administrator “sa” SQL Server account, is created and used to communicate between the DBMS Server and the SolarWinds Platform Server by specifying a new account during the SolarWinds Platform Configuration Wizard.



SolarWinds Configuration Wizard

Database Account

Specify the SQL Server account for Orion to use.

Use a Windows or Azure Active Directory account to access the database.

○ Use an existing account

Existing Account:

Password:

Use a SQL Server account to access the database.

● Create a new account

New Account: SolarWindsOrionDatabaseUser

Password: ************

Confirm Password: ************

○ Use an existing account

Existing Account: SolarWindsOrionDatabaseUser

Password: ************

4. Administrators of the IT systems running the Microsoft SQL Server software must ensure that the Transparent Data Encryption mechanism of SQL Server is enabled on databases storing TSF Data to encrypt data at rest by following these steps:
    a. Create a master key.
    b. Create or obtain a certificate protected by the master key.
    c. Create a database encryption key and protect it by using the certificate.
    d. Set the database to use encryption.

    The following SQL commands example shows encryption and decryption of the ExampleDatabase database using a certificate named MyServerCert that's installed on the server.

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD =
'<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My
DEK Certificate';
GO
USE ExampleDatabase;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
```

```
GO
ALTER DATABASE ExampleDatabase
SET ENCRYPTION ON;
GO
```

5. Administrators of the IT systems running the Microsoft SQL Server software must restrict remote access to the host running Microsoft SQL Server, by applying rules to Windows Firewall (or other firewall software/hardware protecting the host) to limit DBMS Server listener port (i.e., TCP 1433) connections to be established only between hosts running TOE components and the DBMS Server.
6. Administrators of the IT systems running the Microsoft SQL Server software must ensure that access to the Microsoft SQL Server software and data files is limited only to trusted domain or operating system users. This ensures that TSF data is secure and follows the best practices around granting account access with least privileges.
7. SolarWinds recommends using a certificate issued by a trustworthy Certificate Authority as well as securing communication between the SQL Server and the SolarWinds Platform server by enabling TLS functionality and setting the firewall settings to allow connections to be made only between the SQL Server Host and SolarWinds Platform server.

4. Acceptance Procedures

The acceptance procedures by the TOE's users includes the following four steps.

1) Verify the product components' licenses have been posted and verify the correct version of the *SolarWinds Hybrid Cloud Observability for Federal Government 2024.2.1 Common Criteria Supplement* has been downloaded.
2) Download the TOE file for installation and verify the download integrity.
3) Install the executable and verify their correct versions.
4) Download the 14 SolarWinds user guidance documents and verify their versions.

The TOE supports any number of SolarWinds Platform Severs with any number of instances of the 12 product components (IPAM, LA, NCM, NTA, NPM, SAM, SCM, SRM, UDT, VMAN, VNQM, and WPM). The TOE must include one instance of EOC on the EOC Server. The following sections describe installation of a minimum TOE: one SolarWinds Platform Server supporting the 12 product components and one EOC Server supporting EOC. However, the following installation instructions can be used to expand to a distributed installation.

4.1 The SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 Common Criteria Supplement

The first step in installing the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 Common Criteria evaluated product is for the end user to logon to the SolarWinds Customer Portal with their established credentials and verify the 13 licenses have been posted for the 13 product components or a single Hybrid Cloud Observability licenses along with separate SRM and WPM licenses have been posted. If the licenses have not been posted, the end user should contact SolarWinds Support for assistance.

End users can verify they have the correct version of the *SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 Common Criteria Supplement* by comparing the product components' names and version numbers listed in the supplement to the versions listed.on the SolarWinds Common Criteria Webpage.

4.2 Downloading the TOE file for Installation and Verifying the Download Integrity

The next installation step is for the user to navigate to the SolarWinds Common Criteria Webpage and download the installation file. The file is available by selecting the URL listed on the webpage. The installation files, Solarwinds-CC-OOAE-2024.2.1-OfflineInstaller.iso and Solarwinds-CC-EOC-2024.2.1-OfflineInstaller.iso , contains the 13 product components (EOC, IPAM, LA, NCM, NTA, NPM, SAM, SCM, SRM, UDT, VMAN, VNQM, and WPM).

The user is required to download the both files, one on the SolarWinds Platform Server and one on the EOC Server. The EOC product component can only be enabled on a host as the only SolarWinds Platform product.

After downloading each file, the integrity of the two files should be verified by calculating their SHA-256, SHA1, or MD5 hash value and comparing it to the SHA-256, SHA1, or MD5 hash value posted on the SolarWinds Common Criteria Webpage. SolarWinds recommends using SHA-256 algorithm for calculating the hash value before other verification algorithms. If a calculated value does not match the posted value, the user should contact SolarWinds Support for assistance.

4.3 Installing the Executables and Verifying Their Versions

Installation of the two downloads is started by the end user mounting each of the download files and starting installer. Upon selection of the installer file, a short wizard is displayed which allows setting basic settings like installation path and following user through installation of Hybrid Cloud Observability.

Once Hybrid Cloud Observability is installed, the version numbers are displayed at the bottom of the user interfaces: EOC Web Console for the EOC version and SolarWinds Web Console for all other 12 component versions (or HCO and SRM and WPM modules when enabled). End users can verify they have the correct version of the TOE's product components by comparing the versions listed on the console's interfaces to the versions listed on the SolarWinds Common Criteria Webpage. If the versions do not match, the installer should contact SolarWinds Support for assistance.

4.4 Downloading the SolarWinds User Guidance and Verifying Their Versions

The last step in the installation process is to download the 14 SolarWinds user guidance documents. The SolarWinds Common Criteria Webpage contains a list of each of the 13 product components and includes a link that enables the end user to download the appropriate Administrator Guides for each product component (the SAM component includes two documents) and the SolarWinds Platform.

The following table displays the names and version numbers of the 14 SolarWinds user guidance documents.

Table 1 - Guidance Documentation

Prod Comp	Document Name	Version
EOC	*SolarWinds® Enterprise Operations Administrator Guide*	Version 2024.2
IPAM	*SolarWinds® IP Address Manager Administrator Guide*	Version 2024.2
LA	*SolarWinds® Log Analyzer Administrator Guide*	Version 2024.2
NCM	*SolarWinds® Network Configuration Manager Administrator Guide*	Version 2024.2
NPM	*SolarWinds® Network Performance Monitor Administrator Guide*	Version 2024.2
NTA	*SolarWinds® NetFlow Traffic Analyzer Administrator Guide*	Version 2024.2
SAM	*SolarWinds® Server & Application Monitor Administrator Guide*	Version 2024.2
SAM	*SolarWinds® Server & Application Monitor Getting Started Guide*	Version 2024.2
SCM	*SolarWinds® Server Configuration Monitor Administrator Guide*	Version 2024.2
SRM	*SolarWinds® Storage Resource Monitor Administrator Guide*	Version 2024.2
UDT	*SolarWinds® User Device Tracker Administrator Guide*	Version 2024.2
VMAN	*SolarWinds® Virtualization Manager Administrator Guide*	Version 2024.2
VNQM	*SolarWinds® VoIP and Network Quality Manager Administrator Guide*	Version 2024.2
WPM	*SolarWinds® Web Performance Monitor Administrator Guide*	Version 2024.2
PLATFORM	*SolarWinds® SolarWinds Platform Administrator Guide*	Version 2024.2

Once downloaded, end users can verify they have the correct versions of the 14 SolarWinds user guidance documents by comparing the documents' versions, displayed on the first page of the document, to either the versions displayed on the two running consoles or by comparing the product components' versions listed on the SolarWinds Common Criteria Webpage. The documents' versions should match the product component versions with the possible exception of the maintenance version (third value of the product version number displayed in the form of major.minor.maintenance). The maintenance version may not be present in the guidance documentation. If it's not, the major.minor fields should match the product component's major.minor fields. If the maintenance field is included in the documentation, the complete number should match the product component's version number.

5. Supported Login Methods

The SolarWinds Platform Web Console supports multiple login methods, as described in the "Configure automatic login in the SolarWinds Platform" section of the *SolarWinds Platform Administrator Guide.* The evaluated configuration only supports username and password login performed by SolarWinds Platform. The username and password may be supplied via the login.aspx page or via URL Pass-through.

6. Consolidated role information for SolarWinds Platform

6.1 SolarWinds Platform General info

In the SolarWinds Web Console there is one default accounts: admin

You can then add individual accounts and allow or disallow rights to the following features:

- Administrator rights
- Node management
- Map management
- Report management
- Alert management
- Allow Unmanage objects
- Allow Disable Actions
- Allow Disable Alerts
- Allow Disable All Actions
- View customization

Role	Privileges
Administrator	Read and write access to all areas of the SolarWinds Platform Web Console
User	The administrator sets the individual rights for each user, as listed above.

See the topic "Define what users can access and do in the SolarWinds Platform" on page 527 of the SolarWinds Platform Administrator Guide, v.2024.2. For full information, see the section "Manage SolarWinds Platform Web Console user accounts in the SolarWinds Platform" on page 498.

You can also create Windows or group accounts and set limitations by group.

6.1.1 Parameters for the Administrator

The items in the table below apply to all SolarWinds Platform modules for the SolarWinds Platform Administrator Role. In addition to these settings, you can add specific account limitations to each user to limit their access to a single interface, virtual machine, DataCenter, and so on.

Parameter	User Interface	Purpose	Recommended/Secure values	Warnings/Side effects
Set account enabled	Web Console	Log in immediately	Set Enabled (Disabling an account doesn't delete it).	Disabling an account does not delete it. Account definitions and details are stored in the SolarWinds database and can be enabled later. When you disable an account that was used to create alerts, the alerts' Owner filed is

Parameter	User Interface	Purpose	Recommended/Secure values	Warnings/Side effects
				permanently cleared, but the alerts operate as normal.
Expiration Date	Web Console	Log in temporarily	Specify expiration date	n/a
Disable Session Timeout	Web Console	Log in indefinitely	Session Timeout is set to timeout automatically.	Session timeouts are global. By default, new user accounts are configured to timeout automatically.
Allow Administrator Rights	Web Console	Add and edit user accounts and reset passwords	Don't allow administrator rights for users to change their own passwords.	Granting administrator rights does not assign the Admin menu bar to a user. SolarWinds recommends that you do not allow users to change their own Web Console account passwords.
Allow node management rights	Web Console	Add, edit and delete nodes	Not specified	n/a
Allow map management rights	Web Console	Create, edit and delete maps in the Network Atlas	Not specified	n/a
Allow report management rights	Web Console	Add, edit, schedule and delete reports	Only allow access to some reports, select report category that user can access.	n/a
Allow alert management rights	Web Console	Add, edit and delete alerts	Not allowed. Users with alert management rights have the same privileges	SolarWinds does not recommend enabling Alert Management Rights when a user account is set to expire. When the account expires, any alert the account created behaves erratically. Users with Alert Management Rights have the same privileges as the Administrator of the computer where the SolarWinds Platform is installed.
Allow account to customize views	Web Console	Customize views	Customized view creation is not allowed by default.	n/a

Parameter	User Interface	Purpose	Recommended/Secure values	Warnings/Side effects
Allow account to unmanage objects & Mute Alerts	Web Console	Enable/disable monitoring or stop triggering alerts for monitored entities.	Not specified	Changes made to a view are seen by all other users that have been assigned the same view.
Allow account to clear events, acknowledge alerts and syslogs	Web Console	Acknowledge and clear events, advanced alerts and SysLogs.	Not specified	n/a
Allow browser integration	Web Console	User Additional browser functions, risht click menu options	Not specified	Right-click menu options also depend on installed the SolarWinds Desktop Toolset and running th eToolset Integration Tray application on each client.
Show all available items in breadcrumb list	Web Console	Provide the maximum number of items in the breadcrumb list	Set to ‘0’	n/a
SSH Settings/SSH Access	Web Console	Enables SSH Client for this user.	Not specified	n/a
HTTPS	Configuration Wizard	Select Enable HTTPS and bind to an SSL certificate to enable secure communications with the Web Console	Enable HTTPS	n/a
FIPS	SolarWinds FIPS 140-2 Manager	Runs products using computer security and interoperability standards used by non-military US government agencies and contractors	Enable FIPS	n/a

6.2 EOC-specific

Administrators can specify which SolarWinds Sites the user account can access. They must also associate each EOC user account with a SolarWinds Site account which is used to access SolarWinds Site data. The privileges granted to the associated SolarWinds Site account determine what data the EOC user can view and what actions the user can perform (for example, whether the user can acknowledge alerts in EOC).

Role	Privileges
Administrator	Accounts with administrator privileges are leveraged in order to add a site to EOC. This allows EOC to generate a "system account", establish a connection between EOC and the remote site, and maintain a

	channel of communication. The system account is not visible from the remote site UI and its credentials are encrypted and stored in the EOC database.
User	Additional EOC user accounts configured for access to the new site will utilize this connection. If a user's account has custom credentials, the system account will impersonate the user in order to allow SWIS to apply settings and limitations according to the user's account access rights.

See the topic “SolarWinds Site credentials in EOC” on page 7 of the Enterprise Operations Console Administrator Guide, v2024.2.

6.3 IPAM-specific

When you add a user account in IPAM, you assign the user a role. The role determines the user's privileges.

If subnets are moved to create hierarchy changes, inherited roles are inherited from the new parent. Customized roles are not changed.

Role	Privileges
Administrator	The Administrator user role has read and write access, can initiate scans to all subnets, manage credentials, custom fields, and IPAM settings and has full access to DHCP management and DNS monitoring. Only administrators can perform certain actions, such as: SNMP credentials management Custom fields management Subnet scan settings configuration Directly configure custom roles in the Subnet Edit dialog
Power User	Power Users have the same privileges granted to Operators, with the addition of the following: Draganddrop reorganization of network components in the Manage Subnets and IP Addresses view. Supernet and group properties management, including the ability to edit supernet and group properties and custom fields on portions of the network made available by the Administrator. Initiate scans.
Operator	Operators have the same privileges granted to Read Only users with the addition of the following: Addition and deletion of IP address ranges from portions of the network made available by the site administrator Subnet status selection on the Manage Subnets & IP Addresses page

	IP address property and custom field management, including the ability to edit IP address properties on portions of the network made available by the site administrator
Read Only	This role has read-only access to DHCP servers, scopes, leases, reservations and DNS servers, and zones. This role restricts all access, including access to all DHCP management and DNS monitoring, to the following: All IPAM Web Console widgets, including search and Top XX widgets All IP address and network component properties and custom fields on the Manage Subnets and IP Addresses page The Chart view on the Manage Subnets & IP Addresses page

See the topic "Roles and privileges" on page 21 of the IP Address Manager Administrator Guide, v2024.2.

6.3.1 Parameters for IPAM Roles

The items in the table below apply to specific IPAM roles that can be set in the Web Console.

Parameter	Role	Purpose	Recommended/Secure values	Warnings/Side effects
Full Read/Write access to IPAM functions	IPAM Administrator	When set to Admin, allows full read/write access.	Not specified	n/a
Initiate subnet scans plus read/write access. Full access to DHCP & DNS management	IPAM Power User	Initiate scans to determine network status. Manage DHCP and DNS directly and update servers automatically through the console.	Not specified	n/a
Read/write access to subnets and access to manage DHCP reservations	IPAM Operator	View and edit subnets, plus manage DHCP reservations	Not specified	n/a

6.4 NCM-specific

NCM roles determine what NCM functionality a user or group account can access. By default, user accounts in the SolarWinds Platform do not have access to any NCM functionality.

Role	Privileges
Administrator	This role has unlimited access to NCM functionality, including device configuration management, user account management, and configuration change approvals.
Engineer	This role has Administrator privileges, but cannot view the device configuration transfer status for all users.

WebUploader	This role has read and write access on network devices, but cannot change device configurations without Administrator approval. Can access the Mange My NCM Approval Requests page and view jobs that were created when they scheduled the execution of a config change template. History column does not display link to the job log.
WebDownloader	This role can read and download network device configurations.
WebViewer	This role can only read network device configurations.
None	This is the default role when a user is added to SolarWinds Platform. This role cannot access NCM features and functions.

6.4.1 Parameters for NCM Roles

The items in the table below apply to specific NCM roles that can be set in the Web Console.

Parameter	Role	Purpose	Recommended/Secure values	Warnings/Side effects
Unlimited access to NCM functionality	NCM Administrator	Unlimited access to NCM functionality.	Not specified	n/a
All administrator rights except view config transfer status	NCM Engineer	All Administrator rights except cannot view config transfer status from all users.	Not specified	n/a
Unlimited read/write access to NCM unless Approval system is enabled	NCM WebUploader	Unlimited read/write access unlcess Approval system is enabled.	Not specified	n/a
Read and download network device configurations	NCM WebDownloader	Read access and ability to download network device configurations.	Not specified	n/a
Read network device configurations	NCM WebViewer	View network device configurations	Not specified	n/a

6.5 SAM-specific

Role	Privileges
SAM Administrator	In addition to privileges of the SolarWinds Platform Administrator, allows users to: • Assign application templates to nodes • Modify application templates • Manage and maintain the SAM Credentials Library • Unmanage applications from within the web console

SAM User	Select to allow access to the following: • Real-Time Process Explorer • Service Control Manager • Allow Service Action Rights • Real-Time Event Log Viewer • Allow nodes to be rebooted • Allow IIS Action Rights

6.5.1 Parameters for SAM Roles

The items in the table below apply to the SAM roles that can be set in the Web Console.

Parameter	Role	Purpose	Recommended/Secure values	Warnings/Side effects
Manage SAM-specific entities such as applications and templates	SAM Administrator	Manage SAM-specific entities such as applications and templates	Not specified	n/a
Start/Stop/Restart services	SAM Administrator	Start/stop/restart services	Not specified	n/a
Allow nodes to be rebooted	SAM Administrator	Reboot nodes remotely from the Node Management resource	Not specified	n/a
Allow IIS Action Rights	SAM Administrator	Start/stop/restart Site or Application pool from the Management resources	Not specified	n/a
Real-Time Process Explorer	SAM User	If set to allow, user can view monitored and unmonitored processes for WMI and SNMP monitored nodes.	Do not allow	n/a
Service Control Manager	SAM User	If set to Yes, user can use the Service Control Manager to manage services of monitored Windows nodes, including start, restart, or stop a service. User can also pause polling or provide different credentials for a service.	Set to No	n/a
Allow Service Actions Rights	SAM User	If set to Yes, user can start and stop services.	Set to No	n/a
Real-Time Event Log Viewer	SAM User	If set to Yes, user can view Windows event logs in real-time using the WMI	Set to No	n/a

Parameter	Role	Purpose	Recommended/Secure values	Warnings/Side effects
		protocol, pause and restart polling, log into the selected server with different credentials		
Allows nodes to be rebooted	SAM User	If set to Yes, user can reboot nodes remotely from the Node Management resource	Set to No	n/a
Allow IIS Action Rights	SAM User	If set to Yes, user can start/stop/restart Site or Application pool from the Management resources	Set to No	n/a

6.6 SCM-specific

See "User restrictions in Server Configuration Monitor (SCM)" on page 20 of the v2024.2 administrator guide.

Role	Privileges
SCM Administrator	In addition to the privileges of the SolarWinds Platform Administrator, allows user to: • Set baselines • Access any SCM pages that allow editing o Make changes to profiles o Assign profiles o Change data retention settings
SCM User	SCM users can: • Monitor configuration changes on a node • Compare configurations over time

6.6.1 Parameters for SCM Roles

The items in the table below apply to the SCM roles that can be set in the Web Console.

Parameter	Role	Purpose	Recommended/Secure values	Warnings/Side effects
Manage server configuration profiles, assign profiles to nodes and change server-configuration-specific settings	SCM Administrator	Manage server configuration profiles, assign profiles to nodes and change server-configuration-specific settings such as data retention.	Not specified	n/a

Parameter	Role	Purpose	Recommended/Secure values	Warnings/Side effects
Allow account to set a baseline	SCM Administrator	When set to Yes, user can define or redefine a baseline	Not specified	n/a
Monitor configuration changes on a node	SCM User	User can view configuration changes on a node	Not specified	n/a
Compare configuration changes over time	SCM User	User can view and compare configuration changes over time	Not specified	n/a

7. Caution Concerning Clickjacking

Clickjacking attacks may be launched to trick web users into clicking on web links other than what the user expects or perceives. Administrators are cautioned to verify the destination before invoking a link.

8. Flaw Reports

If a suspected flaw is discovered in SolarWinds Platform, a flaw report may be submitted via the SolarWinds Customer Portal.

After logging on using credentials supplied by SolarWinds, customers may select “Open a Case” to initiate the process of reporting a suspected flaw. After supplying details of the flaw (including SolarWinds Platform log files, error codes, screenshots, exception stacks, etc.), select Submit to create a support case, which notifies the SolarWinds Technical Support organization.

Each time a support case is updated, an email is sent back to the creator (end user or customer). The status may also be checked via the SolarWinds Customer Portal by selecting “Review all Cases”. A summary of all cases created by the current user’s company are displayed. The details of a particular case may be displayed by clicking on a case number in the summary display.

SolarWinds Engineering will work with technical support to troubleshoot, reproduce and accept a flaw and will provide a unique tracking number that is associated to the customer support case for future tracking of the fix.