SolarWinds Hybrid Cloud Observability Software

Security Target

Version 1.6

April 17, 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	June 13, 2023 – Initial release
1.1	August 4, 2023 – Modification based on review results
1.2	October 2, 2023 – Update TOE name and webpage
1.3	October 12, 2023 – Update section 1.6.1
1.4	December 1, 2023 – Update section 3.4
1.5	March 11, 2024 – Update section 3.2.1
1.6	April 17, 2024 – Update ST date

TABLE OF CONTENTS

ACRONYMS LIST

CC	**Common Criteria**
CIDR	**Classless Internet Domain Routing**
CLI	**Command Line Interface**
CLR	**Common Language Runtime**
CPU	**Central Processing Unit**
DBMS	**DataBase Management System**
DHCP	**Dynamic Host Configuration Protocol**
DNS	**Domain Name System**
EAL	**Evaluation Assurance Level**
EOC	**Enterprise Operations Console**
FTP	**File Transfer Protocol**
GB	**GigaByte**
GHz	**GigaHertZ**
GUI	**Graphical User Interface**
HA	**High Availabilty**
HCO	**Hybrid Cloud Observability**
HTTPS	**HTTP Secure**
ICMP	**Internet Control Message Protocol**
IIS	**Internet Information Services**
IMAP	**Internet Message Access Protocol**
IOS	**Internetwork Operating System**
IP	**Internet Protocol**
IPAM	**IP Address Manager**
IT	**Information Technology**
LA	**Log Analyzer**
LUN	**Logical Unit Number**
MAC	**Media Access Control**
MIB	**Management Information Base**
MOS	**Mean Opinion Score**
N/A	**Not Applicable**
NAS	**Network Attached Storage**
NCM	**Network Configuration Manager**
NPM	**Network Performance Monitor**
NTA	**NetFlow Traffic Analyzer**
OS	**Operating System**
POP	**Post Office Protocol**
QoE	**Quality of Expierence**
REST	**Representational State Transfer**
SAM	**Server & Application Monitor**
SCM	**Server Configuration Monitor**
SCP	**Secure CoPy**
SFTP	**Secure FTP**
SLA	**Service Level Agreement**
SNMP	**Simple Network Management Protocol**
SP	**Service Pack**

SQL.....**Structured Query Language**
SRM.....**Storage Resource Monitor**
SSH.....**Secure Shell**
SSL.....**Secure Socket Layer**
ST.....**Security Target**
TCP.....**Transmission Control Protocol**
TFTP.....**Trivial File Transport Protocol**
TOE.....**Target of Evaluation**
ToS.....**Type of Service**
TSF.....**TOE Security Function**
UDP.....**User Datagram Protocol**
UDT.....**User Device Tracker**
URL.....**Uniform Resource Locator**
VMAN.....**Virtualization MANager**
VNQM.....**VoIP & Network Quality Manager**
VoIP.....**Voice over IP**
WAN.....**Wide Area Network**
WMI.....**Windows Management Instrumentation**
WPM.....**Web Performance Monitor**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements, and rationale for the SOLARWINDS® Hybrid Cloud Observability software TOE. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5* and all international interpretations through February 19, 2021. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

SolarWinds Hybrid Cloud Observability Security Target, version 1.6, April 17, 2024.

1.2 TOE Reference

SolarWinds Hybrid Cloud Observability for Federal Government V2022.4.1

The Advanced licensing option includes the following components:

1. SolarWinds Platform V2022.4.1
2. Enterprise Operations Console (EOC) 2022.4.1,
3. IP Address Manager (IPAM) V2022.4.1,
4. Log Analyzer (LA) V2022.4.1,
5. Network Configuration Manager (NCM) V2022.4.1,
6. Network Performance Monitor (NPM) V2022.4.1,
7. NetFlow Traffic Analyzer (NTA) V2022.4.1,
8. Server & Application Monitor (SAM) V2022.4.1,
9. Server Configuration Monitor (SCM) V2022.4.1,
10. Storage Resource Monitor (SRM) 2022.4.1,
11. User Device Tracker (UDT) V2022.4.1,
12. Virtualization Manager (VMAN) V2022.4.1,
13. VoIP & Network Quality Manager (VNQM) V2022.4.1, and
14. Web Performance Monitor (WPM) 2022.4.1

Note that the SolarWinds Platform is automatically installed with the first installed component. The SolarWinds Platform is not a separate product and there is no separate download file for it. The SolarWinds Platform V2022.4.1 is associated with the SolarWinds Server.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5, and augmented by ALC_FLR.2.

1.4 Keywords

Performance Monitor, Configuration Manager, Performance Manager, NetFlow Traffic Analyzer, Address Manager, Quality Manager

1.5 TOE Overview

1.5.1 Usage and Major Security Features

SolarWinds Hybrid Cloud Observability for Federal Government V2022.4.1 is a set of software applications and services executing on one or more Windows servers. The applications monitor a configured set of network-attached devices and applications for status, performance, and

configuration settings. Depending on the size of the network, multiple instances of the applications may be deployed on different servers to provide adequate performance. For enhanced availability and robustness, a failover configuration may be deployed.

SolarWinds Hybrid Cloud Observability for Federal Government V2022.4.1 consists of the following network, application, system, and storage monitoring components:

SolarWinds Platform - SolarWinds Platform is at the core of the SolarWinds IT Management Portfolio. It provides a stable and scalable architecture that includes data collection, processing, storage, and presentation. SolarWinds Platform provides common features like network node discovery, dashboards, reporting, alerting, SNMP traps, Syslog, groups, and more that can be leveraged across all products.

Network Performance Monitor - Network Performance Monitor (NPM) provides the ability to detect, diagnose, and resolve performance issues with a dynamic network. It delivers real-time views and dashboards to visually display network performance. Automated network discovery features enable network managers to keep up with evolving networks.

Server & Application Monitor - Server & Application Monitor (SAM) brings agentless monitoring, alerting, and reporting capabilities to applications and servers. Automatically discovers servers and applications and provides visibility into application performance and the underlying operating systems and servers they run on.

Network Configuration Manager - Network Configuration Manager (NCM) notifies network managers in real-time when device configurations change, helping network managers determine which changes could potentially cause network issues. NCM also provides nightly configuration backups, bulk configuration changes, user tracking, and inventory and compliance reporting.

NetFlow Traffic Analyzer - NetFlow Traffic Analyzer (NTA) enables network managers to quantify exactly how a network is being used, by whom, and for what purpose. The application mapping feature correlates the traffic arriving from designated ports, source IPs, destination IPs, and protocols to application names network managers can recognize. NTA provides a comprehensive view of the network traffic, enabling network managers to find the bottlenecks or identify the bandwidth hogs.

IP Address Manager - IP Address Manager (IPAM) is an IP address management component that enables network managers to create, schedule, and share IP address space reports. IPAM provides IP address management that is unified with performance monitoring data for a comprehensive view of network health.

VoIP & Network Quality Manager - VoIP & Network Quality Manager (VNQM) delivers a network and VoIP monitoring solution for identifying site-specific and WAN-related performance issues from the perspective of each of the remote sites. With this component, network managers can utilize Cisco IP SLA technology with automatic VNQM setup to monitor key WAN performance metrics, including Cisco VoIP jitter and MOS.

User Device Tracker - User Device Tracker (UDT) delivers automated user and device tracking to monitor who and what are connecting to the network. Searches of the accumulated information can be performed on a user name, IP address, Hostname, or MAC address.

Log Analyzer - Log Analyzer (LA) continuously collects, consolidates, and manages all network, infrastructure, and application logs. Log sources such as syslog, SNMP traps, and

Windows Event logs are stored, aggregated, tagged, and indexed for search allowing an administrator a unified view and full visibility into the performance of their IT environment.

Web Performance Monitor - Web Performance Monitor (WPM) continuously monitors the performance of web servers and applications. Performance issues can be identified as DNS look-up, connection time, send time, time to first byte, or content download time.

Server Configuration Monitor - Server Configuration Monitor (SCM) notifies systems administrators in real-time when server and application configurations change, helping systems administrators determine which changes could potentially cause systems issues. SCM provides hardware and installed software inventory tracking, custom file and Windows registry monitoring, baseline tagging, and line-by-line comparison of configuration over time.

Storage Resource Monitor - Storage Resource Monitor (SRM) continuously monitors the status and performance of multi-vendor storage environments. Performance issues can be identified for NAS and SAN storage components as well as more granular entities such as volumes and storage pools.

Virtualization Manager - Virtualization Manager (VMAN) delivers integrated VMware vSphere® and Microsoft® Hyper-V® recommendations, capacity planning, performance monitoring, VM sprawl control, VDI performance monitoring, configuration management, and alert remediation. VMAN provides a dashboard view of the health and status of applications, as well as all dependent virtual server, host, cluster, and datastore information that supports the application and its virtual server.

Enterprise Operations Console - Enterprise Operations Console (EOC) provides a consolidated command center to remotely monitor critical network infrastructure in multiple different physical locations. EOC provides a consolidated command center to monitor the entire enterprise network and gives network managers unified visibility into remote SolarWinds servers.

HCO provides the following capabilities to network managers:

- Schedule network scans to identify new network devices or applications.
- Perform detailed monitoring & analysis of performance data from routers, switches, servers, and applications to identify peak performance issues.
- Monitor the health of critical applications.
- Remotely monitor WMI performance counters to identify and resolve application issues.
- Monitor the availability and responsiveness of critical DNS, IMAP4, and POP3 network services.
- Get a comprehensive view of network traffic on a single page, or drill down into any element’s traffic.
- Break down the display of network traffic information by application.
- Identify network issues across the enterprise.
- Perform detailed collection, aggregation, and analysis of log data, faults, and events from network devices, servers, and applications.

- Configure alerts for correlated events, sustained conditions, or complex combinations of device states.
- Generate reports for network performance, application performance, and server availability.
- Schedule and automatically backup network device configurations on a regular basis for routers, switches, firewalls, and wireless access points.
- Receive real-time alerts when configurations change on monitored resources.
- Generate a detailed network inventory of all managed devices, including serial numbers, port details, and IP addresses.
- Generate a detailed server and operating system inventory of all managed devices, including serial numbers, hardware configuration, and installed software.
- Perform remote IOS/firmware updates in real time or schedule them to run at a future time.
- Generate configuration change reports for monitored resources.
- Establish unique accounts and specify which types of information are displayed for a particular user.

Users may interact with the TOE via multiple interfaces. The EOC Web Console provides access to the EOC, and through it provides visibility to the overall TOE, which is especially useful when multiple SolarWinds Servers are deployed. The SolarWinds Web Console provides access to individual SolarWinds Servers. All of these interfaces support connections from remote IT systems via web browsers.

User access to information via each of these interfaces is controlled by the roles configured for individual users by administrators. When a connection is established, the user is prompted for a username and password. User credential validation is performed by the TOE for the SolarWinds Web Console interface, and by Windows for the EOC Web Console interface. In all cases, permitted user accounts must be defined within the TOE so that user-specific TOE parameters (e.g. role) can be associated with each user.

1.5.2 TOE type

Network and Network Related Devices and Systems

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of applications installed on multiple server types:

1. EOC Server - EOC installed on a dedicated server.
2. SolarWinds Server - HCO components (other than EOC) installed on a dedicated server. Any combination of components may be installed with each instance. Any combination is generically referred to as a SolarWinds Server.

Table 1 - EOC Server Minimum Requirements

Item	Requirements
Operating System	Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022
Web Server	Microsoft IIS Version 8.5 or later
.NET Framework	Version 4.8 or later
CPU	Quad-core processor 3 GHz
Memory	32 GB
Available Disk Space	60 GB
DBMS	Microsoft SQL Server 2016 SP1, 2016 SP2 Microsoft SQL Server 2017 Microsoft SQL Server 2019 Microsoft SQL Server 2022

The hardware requirements for EOC Servers satisfies operational environments of up to 60 SolarWinds Servers with up to 1,200,000 managed elements in total from all attached SolarWinds sites. To support a larger number of managed elements or SolarWinds Servers, users should contact SolarWinds for scaling requirements.

Table 2 - SolarWinds Server Minimum Requirements

Item	Requirements
Operating System and Web Server	Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022
Web Server	Microsoft IIS version 8.5 or later
.NET Framework	Version 4.8 or later ASP .NET 2.0 Ajax Extension, Version 1 or later
SNMP Trap Services	Windows operating system management and monitoring tools
CPU	Octa-core Processor 3 GHz or better
Memory	32 GB
Disks	2 x 146 GB 15K Hard Drives (RAID 1/Mirrored Settings)
TFTP Server	SolarWinds TFTP Server 11.2.1.60010

The hardware requirements for SolarWinds Servers satisfy operational environments of up to 1,000,000 managed elements. To support a larger number of managed elements, users should contact SolarWinds for scaling requirements.

In addition to these platforms, the database used by the SolarWinds Server is installed on a dedicated server. Each SolarWinds Server requires its own Database Server.

Table 3 - Database Server Minimum Requirements

Item	Requirements
DBMS	Microsoft SQL Server 2022, 2019, 2017, 2016 SP1, 2016 SP2 Express, Standard, or Enterprise.

Item	Requirements
Operating System	Microsoft Windows Server 2016 Microsoft Windows Server 2019
Additional Software	SQL Server System Common Language Runtime (CLR) Types Microsoft SQL Server Native Client Microsoft SQL Server Management Objects
CPU	Dual Quad Core 3 GHz
Memory	64 GB
Available Disk Space	40 GB

The hardware requirements for Database Servers are determined by the DBMS being used.

Browser sessions connecting to any of the servers are supported using the following minimum versions:

- Microsoft Edge 108 or later
- Firefox 107.0.1 or later
- Chrome 107.0.5304 or later

Credential validation for the EOC Web Console is performed by Windows locally or via Active Directory. The credentials supplied by the user to the TOE are passed to Windows for validation. If credential validation is successful, the same username is used to associate attributes with the user session in the TOE. Credential validation for the SolarWinds Web Console is performed entirely by the TOE.

The evaluated configuration requires that IIS is configured to require secure (HTTPS) connections on all the servers hosting TOE components. This requirement protects any credentials supplied by remote users from disclosure. The SSL functionality is provided by the operational environment.

1.6 TOE Description

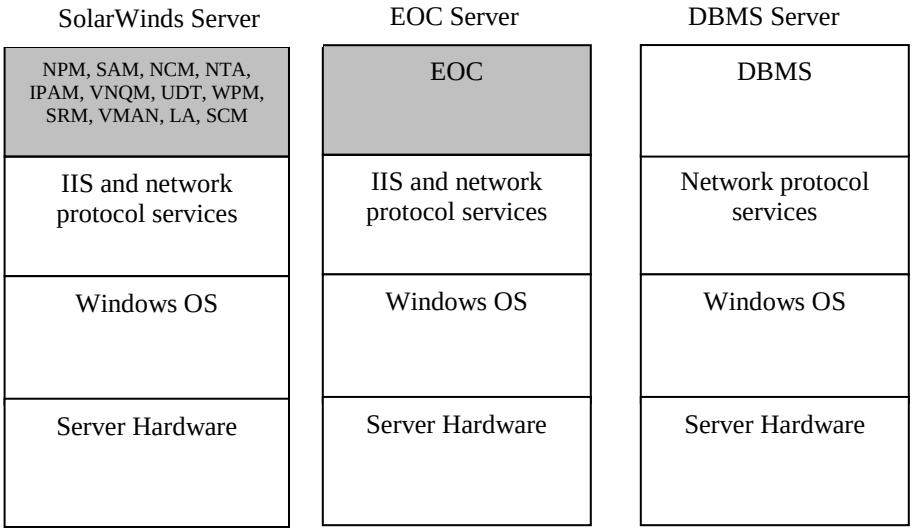
HCO acts as a monitoring and management tool for use by network managers. It maintains a list of the managed elements in the network, monitors their operation, and alerts the network managers to specified conditions. Managed elements are network devices (e.g. routers and switches), servers, storage devices, or applications that can be monitored by standard mechanisms such as SNMP, ICMP, Syslog, or WMI. NCM functionality may be used to track configuration changes on the network devices for products that are able to download a copy of their current configuration parameters. SCM functionality may be used to track configuration changes on servers and applications via the SolarWinds Agent.

Users interact with the TOE via multiple mechanisms. The EOC Web Console and SolarWinds Web Console are provided for remote interaction with the EOC and HCO functionality.

1.6.1 Physical Boundary

The TOE consists of the SolarWinds components identified in Section 1.2 executing on multiple dedicated Windows servers. The TOE is depicted in Figure 1, with TOE components shaded. The operating systems (including the network protocol stacks and cryptographic functionality), web servers, and DBMS are outside the TOE boundary.

Figure 1 - Physical Boundary



The SolarWinds Engineer's Toolset distributed as part of HCO is not installed in the evaluated configuration and is not included in the physical boundary. All other TOE components mentioned in the table below are distributed with the standard distribution mechanisms and are included in the TOE boundary. The TOE components are available to end users via downloading the files made available from the SolarWinds Common Criteria Website. The file, Solarwinds-CC-OOAE-2022.4.1-OfflineInstaller.iso, contains the 12 product components executables (IPAM, LA, NCM, NTA, NPM, SAM, SCM, SRM, UDT, VMAN, VNQM, and WPM). The file, Solarwinds-CC-EOC-2022.4.1-OfflineInstaller.iso contains the EOC product component executables.

The following table identifies the TOE's components.

Table 4 - TOE Component Download Files

Component Acronym	Component Name	Version
Contents in the Solarwinds-CC-EOC-2022.4.1-OfflineInstaller.iso file		
N/A	SolarWinds Platform	2022.4.1
EOC	Enterprise Operations Console	2022.4.1
Contents in the Solarwinds-CC-OOAE-2022.4.1-OfflineInstaller.iso file		
N/A	SolarWinds Platform	2022.4.1
IPAM	IP Address Manager	2022.4.1
LA	Log Analyzer	2022.4.1
NCM	Network Configuration Manager	2022.4.1
NPM	Network Performance Monitor	2022.4.1
NTA	NetFlow Traffic Analyzer	2022.4.1
SAM	Server & Application Monitor	2022.4.1
SCM	Server Configuration Monitor	2022.4.1
SRM	Storage Resource Monitor	2022.4.1
UDT	User Device Tracker	2022.4.1
VMAN	Virtualization Manager	2022.4.1

Component Acronym	Component Name	Version
VNQM	VoIP & Network Quality Manager	2022.4.1
WPM	Web Performance Monitor	2022.4.1

The following Windows services and stand-alone servers are sub-components of the HCO TOE component, upon SolarWinds Platform installed, all the sub-components will add themselves as Windows Services which are designed to run continuously in the background.

- SolarWinds Administration Service 2022.4.1.2010
- SolarWinds Agent 2022.4.2010.1
- SolarWinds MIBs 1.3.0.50051
- SolarWinds Platform 2022.4.1.2010
- SolarWinds SCP Server 2.2.0.60035
- SolarWinds TFTP Server 11.2.1.60010
- SolarWinds Web Performance Monitor Recorder 2022.4
- SolarWinds Web Performance Monitor Transaction Player 2022.4.1

The physical boundary includes the following guidance documentation in their latest version (with the corresponding document file name):

1. ***SolarWinds® Hybrid Cloud Observability for Federal Government Version 2022.4.1 Common Criteria Supplement Version 1.1*** **(**SolarWinds HCO CC Supplement v1.1.pdf**)**
2. *SolarWinds® Platform Administrator Guide Version 2022.4 (orion_platform_2022-4_administrator_guide.pdf)*
3. *SolarWinds® Enterprise Operations Console Administrator Guide Version 2022.3* (eoc_2022-3_administrator_guide.pdf)
4. *SolarWinds® Network Performance Monitor Administrator Guide Version 2022.4* (npm_2022-4_administrator_guide.pdf)
5. *SolarWinds® Server & Application Monitor Administrator Guide Version 2022.4.1* (sam_2022.4.1_administrator_guide.pdf)
6. *SolarWinds® Network Configuration Manager Administrator Guide Version 2022.4* (orionncmadministratorguide_2022-4.pdf)
7. *SolarWinds® IP Address Manager Administrator Guide Version 2022.4* (ipam_2022-4_administrator_guide.pdf)
8. *SolarWinds® NetFlow Traffic Analyzer Administrator Guide Version 2022.4* (nta_2022-4_administrator_guide.pdf)
9. *SolarWinds® User Device Tracker Administrator Guide Version 2022.4* (udt_2022-4_administrator_guide.pdf
10. *SolarWinds® VoIP and Network Quality Manager Administrator Guide Version 2022.4* (vnqm_2022-4_administrator_guide.pdf)

11. *SolarWinds® Log Analyzer Administrator Guide Version 2022.4.1* (la_2022-4-1_admin_guide.pdf)
12. *SolarWinds® Web Performance Monitor Administrator Guide Version 2022.4* (wpm_2022.4_administrator_guide.pdf)
13. *SolarWinds Server Configuration Monitor Administrator Guide Version 2022.3* (scm_2022-3_administrator_guide.pdf)
14. *SolarWinds Storage Resource Monitor Administrator Guide Version 2022.4* (srm_2022-4_administrator_guide.pdf)
15. *SolarWinds® Virtualization Manager Administrator Guide Version 2022.4* (vman_2022-4_administrator_guide.pdf)

All guidance documentation is distributed as PDF files available from links on the SolarWinds Common Criteria Webpage.

Important Notices Concerning Common Criteria Supplement Document Usage

Common Criteria Supplement, refer item 1 above, provides guidance to the user to install and use the SolarWinds Hybrid Cloud Observability for Federal Government Version 2022.4.1 in accordance with the evaluated configuration specified for the Common Criteria evaluation. When any guidance needed during using this CC evaluated version, the user should refer to this supplement document along with other guidance documents listed in the SolarWinds Common Criteria Webpage. And if there was any conflict between this supplement document and any other guidance doc, Common Criteria Supplement Document should be followed to stay in certified configuration and scope.

1.6.2 Logical Boundary

The TOE provides the following security functionality:

1. Audit - Audit records are generated for specific actions performed by users. The audit records are stored in the SolarWinds database and may be viewed via the SolarWinds Web Console by authorized administrators.
2. Identification and Authentication – When a connection is established to the EOC Web Console or SolarWinds Web Console, the TOE prompts the user for login credentials. The credentials are validated by the TOE for the SolarWinds Web Console. For the EOC Web Console, the credentials are first passed to Windows for validation.
3. Management – There are different TOE security function data for different TOE components, such as specific for NCM, IPAM and SCM etc. The management functionality provides multiple management access mechanisms for users. For each specific TOE security function data, dedicated access table will be established, the security function data privileges for the users vary based upon the definition. Individual user's access right for each TOE component security function data is determined by the user's role of each TOE component.
4. Network Monitoring – The status and performance of managed elements are monitored. The results are saved and may be viewed by authorized users. Access to data about the managed elements may be limited by view limitations. Alerts may be generated to notify network managers of configured conditions detected about the managed elements.

Conditions detected by HCO include element status changes and performance threshold values being exceeded.

5. Network Configuration Management – The configurations of network devices may be downloaded from the network device, saved in the TOE database, and compared to a reference configuration. If a configuration change is detected, an upload of a saved configuration for the network device may be triggered.
6. Server Configuration Management – The configurations of servers, windows registry, and applications may be collected via SolarWinds Agent, saved in the TOE database, and compared to a reference configuration.

1.7 Functionality Excluded from the Evaluation

The following functionality provided by SolarWinds Hybrid Cloud Observability for Federal Government V2022.4.1 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 Web Console views.
- The “Check for product updates” function is not used.
- Custom device pollers are not configured. HCO 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 HCO installations there are no custom pollers configured. HCO 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 with the TOE are under evaluation.
- Custom component monitors are not configured. HCO 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 HCO installations there are no custom component monitors configured. Component monitors supplied by SolarWinds with the TOE 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. HCO 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 clean HCO installations there are no custom NCM device templates. The default device templates supplied by SolarWinds with the TOE are under evaluation.

- Customized SCM custom profiles are not configured. Similar to NCM device templates, the SolarWinds platform allows users 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 with the TOE is under evaluation.
- Customized views are not configured on SolarWinds Web Consoles. HCO allows the 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). By default, in clean HCO installations there are no customized views configured. The default views supplied by SolarWinds with the TOE are used and under evaluation.
- View Limitations are not configured. HCO 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 Web Consoles. HCO has the capability to configure account limitations, similar to view limitations (apply to a specific view only), and it will restrict displayed devices for a user on all views (pages). By default, on clean installations 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. EOC allows users to create their own customized views. By default, in clean EOC installation there are no customized views configured. The default views supplied by SolarWinds with the TOE 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 HCO. Otherwise, HCO 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 that runs the TOE are under evaluation.(more detail on it).
- Alert Limitations are not configured. Similar to other limitations (view limitation and account limitation), this functionality will limit access (view or edit) to alerts for specific users. By default, such limitations are not configured.
- Alert Custom Properties are not configured. HCO has a concept of Custom Properties that are additional fields which can describe better monitored objects, such as responsible

team, business unit, owner in organization etc. Those fields can be created by customer via SolarWinds 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 HCO installations.

- Advanced Alert Options are not configured. HCO provides a wizard for guiding users through the 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. 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.
- 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.
- HCO supports the use of SFTP and SCP to upload files containing security information from monitored devices. This functionality is excluded from the evaluation.
- Validation of web interface user credentials is performed by HCO. Validation by an LDAP server is not configured. HCO has a functionality that allows to use Windows Authentication with Active Directory for authentication. Not configured by default.
- SolarWinds 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. Management of the TOE is performed via the GUI.
- UDT provides the ability to send commands to network devices to shut down a port. This functionality is excluded from the evaluation.
- SolarWinds Engineer's Toolset component is not installed or used. This Engineer's Toolset helps users monitor and troubleshoot the network with the most trusted tools in network management, such as Response Time Monitor, Interface Monitor, CPU Monitor, Memory Monitor, and TraceRoute (https://www.solarwinds.com/engineers-toolset).
- The SAML is not configured for SSO and it's not included in the evaluation.

1.8 TSF Data

The following table describes the TSF data. The term Node is used to describe any network device monitored by the TOE.

Table 5 - TSF Data Descriptions

TSF Data	Description
Data Related to SolarWinds Servers or SolarWinds Web Console	
Alert Configuration	Defines the conditions for generating Alerts, which may be triggered by the occurrence of an event or by the crossing of a threshold value for a monitored element. Attributes include: • Name • Enabled or disabled • Frequency • Severity • Trigger and reset conditions • Time of day limitations • Actions, including notification destinations
Alerts	The set of Alerts that have been generated as a result of the Alert Configurations. Alerts are not shown by default once they have been acknowledged by an authorized user.
Application Monitor Templates	Define a group of component monitors modeling the total availability and performance level of an application. Attributes include: • Polling frequency • Polling timeout • Associated Component Monitors
Assigned Application Monitors	Define the assigned component monitors that are run at regular intervals, and then the status results from the component monitors are used to determine an overall status for an application.
Assigned Component Monitors	Define the assignment of application monitor templates to Network Devices hosting an application to be monitored.
Audit Trail Retention	Specifies the number of days that audit records are retained.
CLI Credential Sets	Define credentials used to communicate with Network Devices via Telnet or SSH to configure IP SLA Operations or obtain information about DHCP configurations.
Component Monitors	Define the mechanisms used to monitor the status and performance of an aspect of an application. Attributes include: • Protocol used to poll information concerning the application
Events	The set of Events that have occurred regarding managed elements, such as an interface status changing to up or down. Events are not shown by default once they have been cleared by an authorized user.
Groups	Defines groupings of Network Devices, enabling the corresponding set of Network Devices to be selected for an operation. Groups may be used to create a hierarchical grouping of the Network Devices.
IPAM Addresses and Subnets	Define the IP address ranges or subnets that are monitored by the IPAM functionality. Attributes include: • Name • Address range or CIDR prefix • Scan interval • Automatic Scanning enabled/disabled

TSF Data	Description
IPAM DHCP Scopes	Define the DHCP scopes configured in Cisco IOS and Microsoft DHCP servers that are monitored by the IPAM functionality. Parameters include: • Address range • DHCP Server • Scan parameters • Leases
IPAM DHCP Servers	Define the DHCP servers to be monitored. Parameters include: • IP address/Name • Monitoring protocols supported • Served scopes • Address usage
IPAM DNS Servers	Define the DNS servers to be monitored. Parameters include: • IP address/Name • Monitoring protocols supported • Configured zones
IPAM DNS Zones	Define the DNS zones configured in DNS servers that are monitored by the IPAM functionality. Parameters include: • Zone name • Zone members • DNS Server • Scan parameters
IPAM Settings	Define the operation of IPAM monitoring. Parameters include: • Subnet scan parameters • Device CLI credentials for Scope scans • Device SNMP credentials for Scope scans
NCM Compliance Report Configurations	Define the set of pattern searches that can be applied to configuration files to detect configured conditions. Properties include: • Name • Description • Rules (Patterns to search for, along with severities) • Policies (Collections of Rules)
NCM Compliance Reports	Results of NCM Compliance Report Configurations applied to specific NCM Nodes.
NCM Config Change Templates	Define scripts that can be executed on Nodes to perform common configuration functions. Attributes include: • Name • Description • Tags • Parameters for variables used in the script • Script commands
NCM Default Communication Parameters	Define the default parameters used when communicating with a managed Node. Parameters include: • Community String • SNMPv3 Settings • Login Information • Transfer Protocols • Transfer Ports

TSF Data	Description
NCM Device Configuration Files	Contains the configuration information for a Node. This information may be obtained via download from a Node or by editing an existing configuration file. Configuration files may be designated as baseline configurations for a Node.
NCM Ignore List	Specifies a set of entities that are not added as Managed Devices even if they are found during discovery processes.
NCM Inventory Settings	Specify the statistics collected from Nodes during Inventory Jobs.
NCM Jobs	Define jobs configured to perform periodic operations against Nodes, such as downloading a configuration file or collecting inventory information. Parameters include: • Name • Type of job • Starting date/time • Ending date/time • Frequency • Windows credentials for local job execution • Selected Nodes • Download configuration file parameters • Command script • Results parameters
NCM Settings	Define the behavior of NCM with regard to change detection for Node configurations. Settings include: • Realtime Change Detection • Enable Realtime Config Change Notifications • Configuration Comparison Parameters • Syslog Receiver Parameters • SNMP Trap Receiver Parameters
NetFlow Sources	Define the interfaces in Network Devices that are monitored by the NTA functionality.
Network Devices	Defines the set of Network Devices monitored by the TOE. Attributes include: • Hostname or IP Address • Dynamic IP Address • Monitor via ICMP only • External (applications are monitored, but not the device itself) • VMware parameters, including credentials • SNMP parameters, including credentials • Polling parameters • Management State (polled or not polled) • Interfaces • Interface Management Parameters (polled or not polled, what parameters are polled, alert when down, bandwidth) • Applications • Whether the Device is monitored by VNQM and/or NCM • SNMP Version • SNMP Parameters • Login Type (Device or User) • Device Login Credentials • Communication Protocols and Ports

TSF Data	Description
NTA Settings	Define the operation of NTA monitoring. Parameters include: • Enable automatic addition of NetFlow sources • Enable data retention for traffic on unmonitored ports • Allow monitoring of flows from unmanaged interfaces • Application and Service Ports • Enable/disable each Application and Service Port • Limit monitoring to selected Destination or Source IP Address(es) • Monitored protocols • NetFlow collector ports • Types of Services • Name resolution parameters • IP address processing period • Data retention parameters • Chart parameters
Polling Settings	Define the behavior of polling of the managed elements and the amount of time collected data is retained.
Report Configurations	Define the Reports that are generated and made available for review via the SolarWinds Web Console.
Reports	Pre-defined Reports may be viewed via the SolarWinds Web Console.
SAM Settings	Configured information used for monitoring applications. The information includes: • Credential sets • Polling parameters • Data retention policies
SNMP Credential Sets	Define credentials used to communicate with Network Devices via SNMP to obtain information.
SRM Settings	Configured global threshold values used when monitoring storage objects.
SRM Storage Objects	Configured storage objects being monitored. Storage entities include: • Storage Arrays • Storage Pools • LUNs • NAS Volumes • File Shares
Syslogs	The set of Syslog messages that have been received from Network Devices. Syslogs are not shown by default once they have been cleared by an authorized user.
Thresholds	Define values for devices that cause warning or error indicators to be displayed in the SolarWinds Web Console. Threshold values may be set for: • CPU Load • Disk Usage • Percent Memory Used • Percent Packet Loss • Response Time • Availability • Node Warning Interval

TSF Data	Description
Traps	The set of SNMP trap messages that have been received from Network Devices.
UDT AD Domain Controllers	Defines a list of Active Directory Domain Controllers that are monitored for user activity.
UDT Settings	Define the operation of UDT monitoring. Attributes include: • Polling intervals • Data retention periods • Thresholds • Credentials
UDT Watched Entities List	Defines a list of addresses, ports, and names to be tracked.
UDT Whitelist	Defines a list of systems on the network that are considered trusted and a set of rules for adding devices to the list.
User Accounts	Define the user accounts attributes for users authorized to access SolarWinds Servers via the SolarWinds Web Console. Attributes include: • Username • Password • Enabled • Expiration Date • Disable Session Timeout • Allow Administrator Rights (Role) • Allow Node Management Rights • Allow Report Management Rights • Allow Account to Clear Events and Acknowledge Alerts • Alert Sound • Views (restricts access to Views) • Account Limitations • Report Folder (restricts access to Reports) • Menu Bar Assignments (limits access to specific GUIs) • NCM Role • IPAM Role • SAM Role • Allow Account to Unmanage Objects
Views	Define the views that may be invoked by users. Attributes include: • Resources included in the View
VMAN Settings	Configured information used for managing virtualization servers.
VMAN Virtual Servers	Defines a list of virtualization servers that are managed.
VNQM CallManager Nodes	Define the set of Cisco CallManager and CallManager Express devices to be monitored by the VNQM functionality.
VNQM Operations	Define test measurements to be performed by the VNQM functionality on VNQM Nodes. Testing may be configured for DNS, FTP, HTTP, DHCP, TCP Connect, UDP Jitter, VoIP UDP Jitter, ICMP Echo, UDP Echo, ICMP Path Echo, or ICMP Path Jitter. Parameters include: • Measurement type • Frequency • Path type • VNQM Nodes • Warning threshold • Critical threshold

TSF Data	Description
VNQM Settings	Define the operation of VNQM monitoring. Parameters include: • VoIP UDP Port • VoIP Jitter Codec • Test data collection interval • Test data retention period • MOS advantage factor • Type of Service (ToS) octet
VNQM VoIP Nodes	Define the set of VoIP devices that are monitored by the VNQM functionality.
(SolarWinds) Web Console Settings	Defines parameters controlling the behavior of an SolarWinds Web Console session. Settings include: • Session Timeout • Page Refresh Time • Status Rollup Mode
WPM Transaction Monitors	Define a set of HTTP message exchanges to a specified web server. Attributes include: • Sequence of HTTP messages • Target Web Server • Status (e.g., managed) • Timing threshold values
Data Related to EOC or EOC Web Console	
EOC User Accounts	Define the user account attributes for users authorized to access the EOC Web Console. Attributes include: • Username • Role • Accessible SolarWinds Servers • SolarWinds Server Credentials user-supplied or admin-supplied • SolarWinds Server credentials
Menu Bars	Define a set of Views available to a role.
SolarWinds Servers	Define the SolarWinds Servers associated with the EOC. Attributes include: • Name • Hostname or IP Address • URL • SolarWinds Server credentials • Polling interval • Enabled or disabled
Roles	Define the Views members assigned the role may access. Parameters include: • Name • Menu Bar

1.9 Evaluated Configuration

The evaluated configuration consists of the following:

1. One instance of the EOC, installed on a dedicated Windows server.
2. One or more instances of the SolarWinds Server, each installed on a dedicated Windows server. Each SolarWinds Server has NPM, SAM, NCM, NTA, IPAM, UDT, SRM,

WPM, VMAN, SCM, LA, and VNQM installed. For each instance of the SolarWinds Server, a database (and DBMS) is installed on a separate dedicated Windows server.

The following installation and configuration options must be used:

1. IIS on all the dedicated Windows servers hosting TOE 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 SolarWinds Web Console.
4. Enable Audit Trails is selected.
5. Access to the Windows applications to invoke the TOE is restricted in Windows to users authorized to perform those functions, in particular: manage TOE Alerts, and manage Report configuration settings.
6. The Customize option is not configured for any menu bars for the SolarWinds 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 role (Administrator or User).
10. The NTA Database Maintenance option is enabled in order to have the TOE automatically compress and purge data according to the configured periods.
11. When importing User Accounts into the TOE, only individual accounts are imported. Windows Group Accounts are not imported.
12. Only Administrators assign passwords for User Accounts defined in the TOE. Non-Administrators are not permitted to change their own passwords.
13. The SolarWinds Server Browser Integration parameter is not enabled for User Accounts, since the operations performed via this integration are outside the control of the TOE.
14. Custom Configuration Change Templates are not configured or evaluated. The default configuration change templates supplied with the TOE are included in the evaluation.
15. Real-time config change notification is not enabled in NCM since it is dependent on additional software beyond the scope of the evaluated components.
16. Per-device credentials are used rather than per-user device credentials.
17. If TFTP is used to exchange configuration files with Nodes, the TFTP service is restricted to requests from authorized Nodes.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 5, dated April 2017

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2.

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The ST does not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This section defines the nature and scope of the security needs to be addressed by the TOE. Specifically, this chapter identifies:

A) assumptions about the environment,

B) threats to the assets, and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and organisational security policies as P.*policy*.

3.2 Definitions

3.2.1 Assets

All assets to be protected by the TOE are listed in the table as below:

Assets	Description
TSF data	The TSF data such as Audit records, user account and authentication information (Refer to table 5 for the full list of TSF data).
System data	The system data collected from the managed IT system such as status, performance, and configuration settings information. The terms system data and monitor data have the same meaning and are used interchangeably in the ST.

3.2.2 Subjects

The following table lists all subjects that interact with the TOE:

Subject	Description
Threat Agent	An entity that attempting to subvert the operation of the TOE. The goal may be to gain unauthorized access to the assets protected by the TOE. They have public knowledge of how the TOE works and are assumed to possess a low skill level, limited resources to change the TOE configuration settings or parameters and no physical access to the TOE.
Administrator	An authorized user who has unrestricted access to all TOE functionalities. Administrators are responsible for the management of all TOE processes and must ensure that the TOE operates in a secure way (SolarWinds Administrator).
IT Administrator	An authenticated user who is responsible for creating and changed account that are necessary to access the monitored devices.

Authorized user	A user who has been identified and authenticated by the TOE or an identification & authentication mechanism provided by the underlying operating system and accepted by the TOE.
Unauthorized user	An authenticated user but do not have access to the TOE or authorized to perform a certain operation on the TOE.

3.3 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 6 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DBACCESS	Access to the database used by the TOE is well protected by proper configured according to the guidance document and is restricted to use by authorized users.
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
A.NETWORK	There will be a network that supports communication between distributed components of the TOE. This network functions properly.
A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

3.4 Threats

The threats identified in the following subsections are addressed by the TOE and the Operational Environment.

Table 7 - Threats

T.Type	Description
T.INTERCEPT	An unauthorized network entity may monitor and gain access to system data exchanged between the TOE and other IT systems.
T.MASQUERADE	A user or process acting on behalf of a user may masquerade as authorized entity to gain unauthorized access to system data, TSF data, or TOE resources.
T.TSF_COMPROMISE	A user or process acting on behalf of a user may cause compromising of TSF data saved in database as a result of unsophisticated attack, carelessness, willfully negligent or hostile authorized users.
T.UNIDENT_ACTIONS	A user or process acting on behalf of a user may conduct malicious unnoticed actions on TOE, such as unauthorized access to the TOE or unauthorized modification on the TOE configuration. The administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

3.5 Organisational Security Policies

An organisational security policy is a set of rules, practices, and procedures imposed by an organisation to address its security needs.

Table 8 - Organisational Security Policies

P.Type	Organisational Security Policy
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about element or network problems must be applied to data received from managed elements and appropriate notification to users generated.
P.DBMONITOR	The Administrator shall monitor disk space usage of the databases used by the TOE and take proactive steps to protect against data loss. The TOE will be configured to monitor the databases and alert the Administrator to high disk usage levels.
P.DISCLOSURE	Credentials passed between the TOE and remote users will be protected from disclosure.
P.INTGTY	TSF data collected and produced by the TOE shall be protected from modification by any user.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PASSWORDS	Passwords for User Accounts defined in the TOE are only configured by Administrators according to password requirement defined in the guidance documentation.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 9 - Security Objectives for the TOE

O.Type	Description
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit and system data information in a human readable form.
O.CONFIG	The TOE will provide functionality to store, upload, and compare configuration files for administrator-specified network nodes.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.
O.MONITOR	The TOE will monitor the performance and status of the configured Managed Elements and generate alerts when configured conditions are detected.
O.PASSWORDS	The TOE will permit Administrators to configure passwords for User Accounts defined in the TOE. Users may not configure passwords, even for their own account.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 10 - Security Objectives of the Operational Environment

OE.Type	Description
OE.COMM	The Operational Environment will protect communication between the TOE and systems outside the TOE by providing a trusted path, such as encryption channel.
OE.CRYPTO	The Operational Environment will provide cryptographic functionality to protect protocol communications with remote IT systems.
OE.DBACCESS	Those responsible for the TOE must ensure that access to the TOE database is well protected by proper configuring the database according to the guidance document and the access is restricted to authorized users only.
OE.DBMONITOR	The Operational Environment will provide monitoring functionality in order to monitor disk space usage of the database used by the TOE and take proactive steps to protect against data loss. The Administrator will configure TOE to monitor the databases and send alert of high disk usage levels.

OE.Type	Description
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.INSTALL	The Operational Environment will allow Administrator to install and configure the TOE according to the administrator guidance.
OE.INTROP	The TOE is interoperable with the IT Systems it monitors.
OE.NETWORK	The Administrator will install and configure a network that supports communication between the distributed TOE components. he administrator will ensure that this network functions properly.
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going. The TOE will be used by a competent and non-hostile administrator with following the administrator guidance.
OE.SSL	The Operational Environment will require incoming connections to the SolarWinds Web Console and EOC Web Console to use SSL/TLS.
OE.TIME	The Operational Environment will provide reliable timestamps.
OE.WINDOWSACCESS	Users invoking the SolarWinds Server functionality via Windows application programs must successfully perform identification and authentication functions with Windows first, and access to the applications that invoke SolarWinds Server functionality must be limited to users authorized to invoke TOE management functionality.

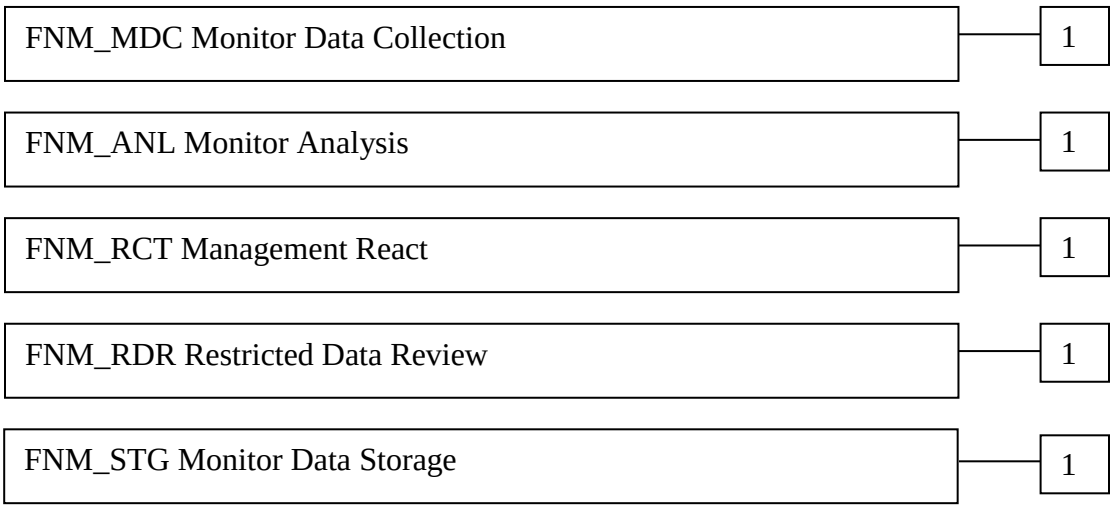
5. Extended Components Definition

5.1 Extended Security Functional Components

5.1.1 Class FNM: Network Management

All of the components in this section are derived from the U.S. Government Protection Profile Intrusion Detection System - System For Basic Robustness Environments.

This class of requirements addresses the data collected and analyzed by network management systems. The audit class of the CC (FAU) was used as a model for creating the IDS class in the Protection Profile, and the IDS class was used as a model for these requirements. The purpose of this class of requirements is to address the unique nature of network management data and provide for requirements about analyzing, reviewing and managing the data. This document uses the term "Monitor data" to refer to the information collected and saved by the collection and analysis functions specified herein.

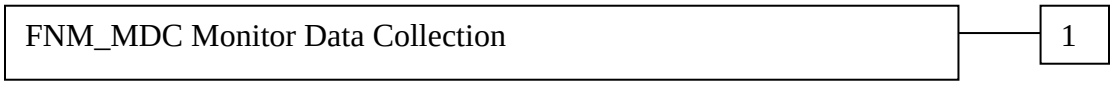


5.1.1.1 FNM_MDC Monitor Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding receipt of information related to the status and performance of managed elements.

Component Levelling:



FNM_MDC.1 Monitor Data Collection provides for the functionality to require TSF controlled processing of data received from managed elements regarding their status or performance.

Management:

The following actions could be considered for the management functions in FMT:

a) Management of the configuration information for real-time feeds.

Audit:

There are no auditable events foreseen.

FNM_MDC.1 Monitor Data Collection

Hierarchical to: No other components.

Dependencies: None

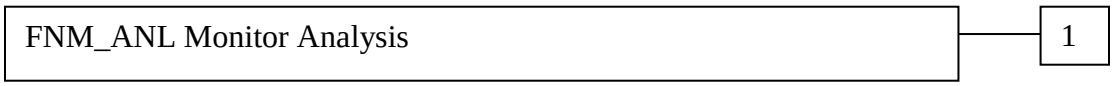
FNM_MDC.1.1 The TSF shall be able to store configuration, status and performance information received via real-time feeds and/or polling.

5.1.1.2 FNM_ANL Monitor Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of information related to status and performance received from managed elements.

Component Levelling:



FNM_ANL.1 Monitor Analysis provides for the functionality to require TSF controlled analysis of data received from managed elements regarding their status or performance.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

FNM_ANL.1 Monitor Analysis

Hierarchical to: No other components.

Dependencies: FNM_MDC.1 Monitor Data Collection

FNM_ANL.1.1 The TSF shall perform the following analysis function(s) on all status and performance information received from managed elements:

a) Status changes;

b) Threshold values exceeded;

c) Configuration changed; and

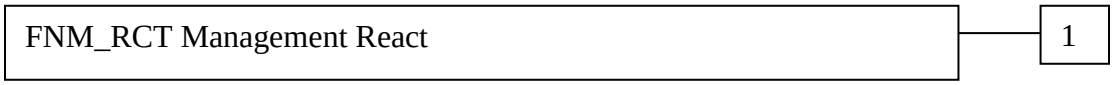
d) Configured conditions satisfied.

5.1.1.3 FNM_RCT Management React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information related to status and performance received from managed elements.

Component Levelling:



FNM_RCT.1 Management React provides for the functionality to require TSF controlled reaction to the analysis of data received from managed elements regarding information related to status and performance.

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

FNM_RCT.1 Management React

Hierarchical to: No other components.

Dependencies: FNM_ANL.1 Monitor Analysis

FNM_RCT.1.1 The TSF shall perform the configured alert notification action(s) when conditions regarding the status or performance of managed elements and specified by an administrator are detected.

5.1.1.4 FNM_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the monitor data collected by the TOE.

Component Levelling:

FNM_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the monitor data collected by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the monitor data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read monitor data that are denied.

b) Detailed: Reading of information from the monitor data records.

FNM_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: FNM_MDC.1 Monitor Data Collection

FNM_ANL.1 Monitor Analysis

FNM_RDR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of Monitor data*] from the Monitor data.

FNM_RDR.1.2 The TSF shall provide the Monitor data in a manner suitable for the user to interpret the information.

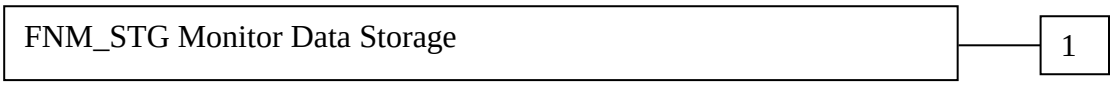
FNM_RDR.1.3 The TSF shall prohibit all users read access to the Monitor data, except those users that have been granted explicit read-access.

5.1.1.5 FNM_STG Monitor Data Storage

Family Behaviour:

This family defines the requirements for the TOE to be able to create and maintain a secure monitor data trail.

Component Levelling:



FNM_STG.1 Guarantee of Monitor Data Availability requires that the monitor data be protected from unauthorised deletion and/or modification.

Management: FNM_STG.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the monitor data storage capability.

Audit: FNM_STG.1

There are no auditable events foreseen.

FNM_STG.1 Guarantee of Monitor Data Availability

Hierarchical to: No other components.

Dependencies: FNM_MDC.1 Monitor Data Collection

FNM_ANL.1 Monitor Analysis

FNM_STG.1.1 The TSF shall protect the stored Monitor data from unauthorised deletion via operations under the control of the TSF.

FNM_ STG.1.2 The TSF shall protect the stored Monitor data from modification via operations under the control of the TSF.

Application Note: Authorised deletion of data is not considered a modification of Monitor data in this context. This requirement applies to the actual content of the Monitor data, which should be protected from any modifications.

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events in the following table*.

Table 11 - Auditable Events

SFR	Event	Details
FAU_GEN.1	Changes to the Enable Audit Trail setting	Old and new setting values
FIA_AFL.1	Unsuccessful login	User account, authentication failure
FIA_ATD.1	User account creation and deletion	User account
FIA_UAU.2	Successful login	User identity, IP address of the remote system
FIA_UID.2	Successful login	User identity, IP address of the remote system
FMT_MTD.1	Modifications to the values of system parameters	Parameter changed, old and new values
	Creation, modification and deletion of monitoring entities (e.g. Node, Application Template)	Action, entity type, entity name, associated Node (if applicable), old and new values (for Node properties)
	Node managed or unmanaged	Action, Node

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the information specified in the Details column of the table above*.

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *all SolarWinds Administrators* with the capability to read *all data* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within *[1-10]* unsuccessful authentication attempts occurs related to *since the last successful authentication of the indicated user identity of SolarWinds Platform Web Console login*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been surpassed, the TSF shall *terminate the session of the user trying to authenticate and block the user account from login until an Administrator defined time period [15 minutes by default] has elapsed.*

6.1.2.2 FIA_ATD.1 User Attribute Definition

Refinement Rationale: The TOE provides multiple access mechanisms for users. The security attributes defined for the users vary based upon the mechanism, with the exception of SolarWinds Windows Applications where the only attribute (the role) is implied. Therefore, iterations for this SFR are specified for individual access mechanisms. The collection of iterations addresses the user attribute definitions for the TOE access mechanisms.

6.1.2.2.1 FIA_ATD.1(1) User Attribute Definition (SolarWinds Web Console)

FIA_ATD.1.1(1) The TSF shall maintain the following list of security attributes belonging to individual users **of the SolarWinds Web Console**:

1. *Username*
2. *Password*
3. *Account enabled status*

4. *Account expiration date*
5. *Allow administrator rights (role)*
6. *Allow Node management rights*
7. *Allow Report management rights*
8. *Allow account to clear Events, acknowledge Alerts and Syslogs*
9. *Alert sound*
10. *Menu Bar assignments*
11. *Report folder*
12. *NCM Role*
13. *IPAM Role*
14. *SAM Role*
15. *SCM Role*
16. *Allow Account to Unmanage Objects*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the SolarWinds Web Console.

6.1.2.2.2 FIA_ATD.1(2) User Attribute Definition (EOC Web Console)

FIA_ATD.1.1(2) The TSF shall maintain the following list of security attributes belonging to individual users **of the EOC Web Console**:

1. *Username*
2. *Role*
3. *Accessible SolarWinds Servers*
4. *SolarWinds Server Credentials user-supplied or admin-supplied*
5. *SolarWinds Server Credentials*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the EOC Web Console.

6.1.2.3 FIA_UAU.2 User Authentication Before any Action

Refinement Rationale: This SFR applies to password validation for the SolarWinds Web Console. Password validation for the EOC Web Console is performed by Windows; Windows is responsible for the complete I&A process for Windows applications that invoke the TOE.

FIA_UAU.2.1 The TSF shall require each **SolarWinds Web Console** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.4 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *dots* to the user while the authentication is in progress.

Application Note: This SFR does not apply to instances when the password is passed to the TOE using URL parameters.

6.1.2.5 FIA_UID.2 User Identification Before any Action

Refinement Rationale: This SFR applies to users accessing the TOE via the SolarWinds Web Console or the EOC Web Console. The TOE does not perform any identification for users accessing the TOE via SolarWinds Windows applications on servers on which SolarWinds Server components are installed. Identification must be performed by Windows prior to the users invoking the applications, as specified in OE.WINDOWSACCESS.

FIA_UID.2.1 The TSF shall require each **SolarWinds Web Console and EOC Web Console** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.6 FIA_USB.1 User-Subject Binding

Refinement Rationale: The TOE provides multiple access mechanisms for users. The security attributes bound to a session for the users vary based upon the mechanism. Therefore, iterations for this SFR are specified for each access mechanism. The collection of iterations addresses the user attribute definition for all TOE access mechanisms.

6.1.2.6.1 FIA_USB.1(1) User-Subject Binding (SolarWinds Web Console)

FIA_USB.1.1(1) The TSF shall associate the following user security attributes with subjects acting on behalf of that **SolarWinds Web Console** user:

1. *Username*
2. *Password*
3. *Account enabled status*
4. *Account expiration date*
5. *Allow administrator rights (role)*
6. *Allow Node management rights*
7. *Allow Report management rights*
8. *Allow account to clear Events, acknowledge Alerts and Syslogs*
9. *Alert sound*
10. *Menu Bar assignments*
11. *Report folder*
12. *NCM Role*
13. *IPAM Role*
14. *SAM Role*
15. *SCM Role*

16. Allow Account to Unmanage Objects

FIA_USB.1.2(1) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **SolarWinds Web Console** users: *attributes are bound from the configured parameters for the identified user account*.

FIA_USB.1.3(1) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **SolarWinds Web Console** users: *User permissions (e.g., Allow administrator rights, NCM Role, IPAM Role) are dynamically retrieved and re-bound as interactions are invoked; Menu Bar assignments are re-bound whenever a Menu Bar parameter is selected by the user; other subject attributes do not change during a session.*

Application Note: Different security attributes are bound for different TOE access mechanisms. This iteration applies to security attributes for users of the SolarWinds Web Console.

6.1.2.6.2 FIA_USB.1(2) User-Subject Binding (EOC Web Console)

FIA_USB.1.1(2) The TSF shall associate the following user security attributes with subjects acting on behalf of that **EOC Web Console** user:

1. *Username*
2. *Role*
3. *Accessible SolarWinds Servers*
4. *SolarWinds Server Credentials user-supplied or admin-supplied*
5. *SolarWinds Server credentials*

FIA_USB.1.2(2) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **EOC Web Console** users: *attributes are bound from the configured parameters for the identified user account*.

FIA_USB.1.3(2) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **EOC Web Console** users: *subject attributes do not change during a session*.

Application Note: Different security attributes are bound for different TOE access mechanisms. This iteration applies to security attributes for users of the EOC Web Console.

6.1.2.6.3 FIA_USB.1(3) User-Subject Binding (SolarWinds Windows Applications)

FIA_USB.1.1(3) The TSF shall associate the following user security attributes with subjects acting on behalf of that **SolarWinds Windows applications** user:

1. *Role (Windows Application Administrator)*

FIA_USB.1.2(3) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **SolarWinds Windows applications** users: *the role is implied by use of the access mechanism*.

FIA_USB.1.3(3) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **SolarWinds Windows applications** users: *subject attributes do not change during a session*.

Application Note: Different security attributes are bound for different TOE access mechanisms. This iteration applies to security attributes for users of the SolarWinds Windows applications. SolarWinds Windows applications are supporting Windows desktop applications that are installed with SolarWinds on the host where TOE is installed. User need certain permission to access them. One example of such applications is WPM Recorder.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MTD.1 Management of TSF Data

Application Note: The TOE provides multiple management access mechanisms for users. The TSF data privileges for the users vary based upon the mechanism. Therefore, iterations for this SFR are specified for each access mechanism. The collection of iterations addresses the TSF data privileges for all TOE access mechanisms. If a TSF data item is not included in the table accompanying the SFR iteration, then no access to that TSF data item is provided via the TOE access mechanism.

6.1.3.1.1 FMT_MTD.1(1) Management of TSF Data (SolarWinds Server TSF Data (Other Than NCM-Specific, SAM-Specific, SCM-Specific and IPAM-Specific))

FMT_MTD.1.1(1) The TSF shall restrict the ability to query, modify, delete, *create, acknowledge* the *SolarWinds Server TSF data (other than NCM-specific, SAM-specific, SCM-specific and IPAM-specific) specified in the following table* to *users with the roles and permissions specified in the following table*.

Application Note: Different TSF data privileges are enforced for different TOE access mechanisms. This iteration applies to TSF data (other than NCM-specific, SAM-specific, SCM-specific and IPAM-specific) for SolarWinds Servers. Access limitations for the NCM-specific, SAM-specific, SCM-Specific, and IPAM-specific data is controlled via an additional security attribute (NCM, SAM, SCM, or IPAM role) assigned to individual user accounts and is addressed in separate iterations of this SFR.

Application Note: SolarWinds Administrators are authorized SolarWinds Web Console user accounts with the Allow Administrator Rights parameter value set.

Table 12 - SolarWinds Server TSF Data Detail

TSF Data	Windows Application Administrator	SolarWinds Administrator	SolarWinds User
Alert Configuration	Query, Modify	None	None
Alerts	None	Query. Acknowledge if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set	Query. Acknowledge if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set
Application Monitor Templates	None	Query and Modify	None
Assigned Application Monitors	None	Query and Modify	None
Assigned Component Monitors	None	Query and Modify	None
Audit Trail Retention	None	Query and Modify	None

TSF Data	Windows Application Administrator	SolarWinds Administrator	SolarWinds User
CLI Credential Sets	None	Query Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set	Query
Component Monitors	None	Query and Modify	None
Events	None	Query. Acknowledge if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set	Query. Acknowledge if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set
Groups	None	Query, Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set	Query
IPAM Settings	None	Query, Create, Modify and Delete	None
LA Jobs	None	Query	None
LA Settings	None	Query, Modify	None
NCM Jobs	None	Query	None
NCM Ignore List	None	Query. Modify if the "Allow Node Management Rights" account parameter is set	Query. Modify if the "Allow Node Management Rights" account parameter is set
NCM Settings	None	Query, Modify	None
NetFlow Sources	None	Query, Create, Modify and Delete	Query
Network Devices	None	Query. Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set	Query. Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set
NTA Settings	None	Query and Modify	None
Polling Settings	None	Query and Modify	None
Report Configurations	Query, Create, Modify and Delete	Query, Create, Modify and Delete if the "Allow Report management" account parameter is set	Query, Create, Modify and Delete if the "Allow Report management" account parameter is set
Reports	None	Query, limited to Reports in the folder configured for the user account	Query, limited to Reports in the folder configured for the user account
SAM Settings	None	Query and Modify	None
SCM Jobs	None	Query	None
SCM Settings	None	Query and Modify	None
SRM Settings	None	Query and Modify	None

TSF Data	Windows Application Administrator	SolarWinds Administrator	SolarWinds User
SRM Storage Objects	None	Query. Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set	Query. Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set
Syslogs	None	Query. Acknowledge if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set	Query. Acknowledge if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set
Thresholds	None	Query and Modify	None
Traps	None	Query	Query
UDT AD Domain Controllers	None	Query, Create, Modify and Delete	None
UDT Settings	None	Query and Modify	None
UDT Watched Entities List	None	Query and Modify	Query
UDT White List	None	Query and Modify	None
User Accounts	None	Query, Create, Modify and Delete	None
Views	None	Query. Modify if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set	Query. Modify if the "Allow Account to Clear Events and Acknowledge Alerts" account parameter is set
VMAN Settings	None	Query, Create, Modify and Delete	Query
VMAN Virtual Servers	None	Query, Create, Modify and Delete	Query
VNQM CallManager Nodes	None	Query, Create, Modify and Delete	Query
VNQM Operations	None	Query, Create, Modify and Delete	Query
VNQM Settings	None	Query, Create, Modify and Delete	None
VNQM VoIP Nodes	None	Query, Create, Modify and Delete	Query
(SolarWinds) Web Console Settings	None	Query and Modify	None
WPM Transaction Monitors	None	Query, Create, Modify and Delete	Query

6.1.3.1.2 FMT_MTD.1(2) Management of TSF Data (NCM-Specific TSF Data on SolarWinds Servers (Accessed via the SolarWinds Web Console))

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, *create*, *execute*, *upload and download* the *NCM-specific TSF data on SolarWinds Servers (accessed via the*

SolarWinds Web Console) specified in the following table to *users with the roles specified in the following table.*

Application Note: Different TSF data privileges are enforced for different TOE access mechanisms. This iteration applies to TSF data specific to NCM functionality on SolarWinds Servers, since access limitations to this information are controlled via a specific security attribute (NCM role) configured for individual user accounts.

Table 13 - NCM-Specific TSF Data Detail

TSF Data	Administrator	Engineer	WebUploader	WebDownloader	WebViewer	None
NCM Compliance Report Configurations	Query, Create, Modify, and Delete	Query, Create, Modify, and Delete	Query, Create, Modify, and Delete	None	None	None
NCM Compliance Reports	Query, Create, Modify, and Delete	Query (no permission to view config transfer status from all users) , Create, Modify, and Delete	Query, Create, Modify, and Delete	None	None	None
NCM Config Change Templates	Query, Create, Modify, Delete, and Execute	Query, Create, Modify, Delete, and Execute	Query, Create, Modify, Delete, and Execute	None	None	None
NCM Default Communication Parameters	Modify	Modify	None	None	None	None
NCM Device Configuration Files	Download, Upload, Query, Modify	Download, Upload, Query, Modify	Download , Upload, Query, Modify	Download, Query	Query	None

6.1.3.1.3 FMT_MTD.1(3) Management of TSF Data (IPAM-Specific TSF Data on SolarWinds Servers (Accessed via the SolarWinds Web Console))

FMT_MTD.1.1(3) The TSF shall restrict the ability to query, modify, delete, *create, and scan,* the *IPAM-specific TSF data on SolarWinds Servers (accessed via the SolarWinds Web Console) specified in the following table* to *users with the roles specified in the following table.*

Application Note: Different TSF data privileges are enforced for different TOE access mechanisms. This iteration applies to TSF data specific to IPAM functionality on SolarWinds Servers, since access limitations to this information are controlled via a specific security attribute (IPAM role) configured for individual user accounts.

Table 14 - IPAM-Specific TSF Data Detail

TSF Data	Admin	Power User	Operator	Read Only
IPAM Addresses and Subnets	Query, Create, Modify, Delete, Scan	Query, Create, Modify, Delete, Scan	Query, Modify	Query
IPAM DHCP Scopes	Query, Create, Modify, Delete, Scan	Query, Create, Modify, Delete, Scan	Query, Modify	Query
IPAM DHCP Servers	Query, Create, Modify, Delete, Scan	Query, Create, Modify, Delete, Scan	Query, Modify	Query
IPAM DNS Servers	Query, Create, Modify, Delete, Scan	Query, Create, Modify, Delete, Scan	Query, Modify	Query
IPAM DNS Zones	Query, Create, Modify, Delete, Scan	Query, Create, Modify, Delete, Scan	Query, Modify	Query
SNMP Credential Sets	Query, Create, Modify, Delete	Query	None	None

6.1.3.1.4 FMT_MTD.1(4) Management of TSF Data (EOC Server TSF Data)

FMT_MTD.1.1(4) The TSF shall restrict the ability to query, modify, delete, *create*, *access* the *EOC Server TSF data specified in the following table* to *users with the roles and permissions specified in the following table*.

Application Note: Different TSF data privileges are enforced for different TOE access mechanisms. This iteration applies to TSF data for EOC Servers.

Table 15 - EOC Server TSF Data Detail

TSF Data	Administrator
EOC User Accounts	Query, Create, Modify, and Delete
Menu Bars	Query, Create, Modify, Delete, and Access
SolarWinds Servers	Query, Create, Modify, Delete, and Access
Roles	Query, Create, Modify, and Delete

6.1.3.1.5 FMT_MTD.1(5) Management of TSF Data (SAM-Specific TSF Data on SolarWinds Servers (Accessed via the SolarWindsWeb Console))

FMT_MTD.1.1(5) The TSF shall restrict the ability to query, modify, delete, *create*, *and scan*, the *SAM-specific TSF data on SolarWinds Servers (accessed via the SolarWinds Web Console) specified in the following table* to *users with the roles specified in the following table*.

Application Note: Different TSF data privileges are enforced for different TOE access mechanisms. This iteration applies to TSF data specific to SAM functionality on SolarWinds Servers, since access limitations to this information are controlled via a specific security attribute (SAM role) configured for individual user accounts.

Table 16 - SAM-Specific TSF Data Detail

TSF Data	Administrator	User
Application Monitor Templates	Query and Modify	Query
Assigned Application Monitors	Query and Modify	Query
Assigned Component Monitors	Query and Modify	Query
Component Monitors	Query and Modify	Query
SAM Settings	Query and Modify	None

6.1.3.1.6 FMT_MTD.1(6) Management of TSF Data (SCM-Specific TSF Data on SolarWinds Servers (Accessed via the SolarWinds Web Console))

FMT_MTD.1.1(6) The TSF shall restrict the ability to query, modify, delete, *create, execute, upload and download* the *SCM-specific TSF data on SolarWinds Servers (accessed via the SolarWinds Web Console) specified in the following table* to *users with the roles specified in the following table*.

Application Note: Different TSF data privileges are enforced for different TOE access mechanisms. This iteration applies to TSF data specific to SCM functionality on SolarWinds Servers, since access limitations to this information are controlled via a specific security attribute (SCM role) configured for individual user accounts.

Table 17 - SCM-Specific TSF Data Detail

TSF Data	Administrator	User
SCM Compliance Report Configurations	Query, Create, Modify, and Delete	Query, Create, Modify, and Delete
SCM Compliance Reports	Query	Query
SCM Config Change Policies	Query, Create, Modify, Delete, and Execute	Query, Create, Modify, Delete, and Execute
SCM Default Communication Parameters	Modify	None
SCM Device Configuration Files	Download, Upload, Query, Modify	Download, Upload, Query, Modify

6.1.3.2 FMT_SMF.1 Specification of Management Functions

Application Note: The TOE provides multiple management access mechanisms for users. Therefore, iterations for this SFR are specified for each access mechanism. The collection of iterations addresses the TSF data management for all TOE access mechanisms.

6.1.3.2.1 FMT_SMF.1(1) Specification of Management Functions (SolarWinds Server Management)

FMT_SMF.1.1(1) The TSF shall be capable of performing the following management functions:

Application Note: This iteration applies to SolarWinds Server management.

Application Note: SolarWinds Administrators are authorized SolarWinds Web Console user accounts with the Allow Administrator Rights parameter value set.

1. *Alert Configuration Management (Query, Modify)*
2. *Application Monitor Templates Management (Query, Modify)*
3. *Assigned Application Monitors Management (Query, Modify)*
4. *Assigned Component Monitors Management (Query, Modify)*
5. *Audit Trail Retention Management (Query, Modify)*
6. *CLI Credential Sets Management (Query, Create, Modify, Delete)*
7. *Component Monitors Management (Query, Modify)*
8. *Groups Management (Query, Create, Modify, Delete)*
9. *IPAM Settings Management (Query, Create, Modify, Delete)*
10. *LA Settings Management (Query, Modify)*
11. *NCM Ignore List Management (Query, Modify)*
12. *NCM Settings Management (Query, Modify)*
13. *NetFlow Sources Management (Query, Create, Modify, Delete)*
14. *Network Devices Management (Query, Create, Modify, Delete)*
15. *NTA Settings Management (Query, Modify)*
16. *Polling Settings Management (Query, Modify)*
17. *Report Configurations Management (Query, Create, Modify, Delete)*
18. *SAM Settings Management (Query, Modify)*
19. *SCM Settings Management (Query, Modify)*
20. *SRM Settings Management (Query, Modify)*
21. *SRM Storage Objects Management (Query, Create, Modify, Delete)*
22. *Thresholds Management (Query, Modify)*
23. *UDT AD Domain Controllers Management (Query, Create, Modify, Delete)*
24. *UDT Settings Management (Query, Modify)*
25. *UDT Watched Entities List Management (Query, Modify)*
26. *UDT White List Management (Query, Modify)*
27. *User Accounts Management (Query, Create, Modify, Delete)*
28. *Views Management (Query, Create, Modify, Delete)*
29. *VMAN Settings Management (Query, Create, Modify, Delete)*
30. *VMAN Virtual Servers Management (Query, Create, Modify, Delete)*

31. *VNQM CallManager Nodes Management (Query, Create, Modify, Delete)*
32. *VNQM Operations Management (Query, Create, Modify, Delete)*
33. *VNQM Settings Management (Query, Create, Modify, Delete)*
34. *VNQM VoIP Nodes Management (Query, Create, Modify, Delete)*
35. *(SolarWinds) Web Console Settings Management (Query, Modify)*
36. *WPM Transaction Monitors Management (Query, Create, Modify, Delete)*

6.1.3.2.2 FMT_SMF.1(2) Specification of Management Functions (NCM Management (Accessed via the SolarWinds Web Console))

FMT_SMF.1.1(2) The TSF shall be capable of performing the following management functions:

Application Note: This iteration specifically applies to NCM functionality management.

1. *NCM Compliance Report Configurations Management (Query, Create, Modify, Delete)*
2. *NCM Config Change Templates Management (Query, Create, Modify, Delete, Execute)*
3. *NCM Default Communication Parameters Management (Modify)*
4. *NCM Device Configuration Files Management (Download, Upload, Query, Modify)*

6.1.3.2.3 FMT_SMF.1(3) Specification of Management Functions (IPAM Management (Accessed via the SolarWinds Web Console))

FMT_SMF.1.1(3) The TSF shall be capable of performing the following management functions:

Application Note: This iteration specifically applies to IPAM functionality management.

1. *IPAM Addresses and Subnets Management (Query, Create, Modify, Delete, Scan)*
2. *IPAM DHCP Scopes Management (Query, Create, Modify, Delete, Scan)*
3. *IPAM DHCP Servers Management (Query, Create, Modify, Delete, Scan)*
4. *IPAM DNS Servers Management (Query, Create, Modify, Delete, Scan)*
5. *IPAM DNS Zones Management (Query, Create, Modify, Delete, Scan)*
6. *SNMP Credential Sets Management (Query, Create, Modify, Delete)*

6.1.3.2.4 FMT_SMF.1(4) Specification of Management Functions (EOC Server Management)

FMT_SMF.1.1(4) The TSF shall be capable of performing the following management functions:

Application Note: This iteration specifically applies to EOC Servers Management.

1. *EOC User Accounts Management (Query, Create, Modify, Delete)*
2. *Menu Bars Management (Query, Create, Modify, Delete, Access)*
3. *SolarWinds Servers Management (Query, Create, Modify, Delete, Access)*
4. *Roles Management (Query, Create, Modify, Delete)*

6.1.3.2.5 FMT_SMF.1(5) Specification of Management Functions (SAM Management (Accessed via the SolarWinds Web Console))

FMT_SMF.1.1(5) The TSF shall be capable of performing the following management functions:

Application Note: This iteration specifically applies to SAM functionality management.

1. *Application Monitor Templates Management (Query, Modify)*
2. *Assigned Application Monitors Management (Query, Modify)*
3. *Assigned Component Monitors Management (Query, Modify)*
4. *Component Monitors Management (Query, Modify)*
5. *SAM Settings Management (Query, Modify)*

6.1.3.2.6 FMT_SMF.1(6) Specification of Management Functions (SCM Management (Accessed via the SolarWinds Web Console))

FMT_SMF.1.1(6) The TSF shall be capable of performing the following management functions:

Application Note: This iteration specifically applies to SCM functionality management.

1. *SCM Compliance Report Configurations Management (Query, Create, Modify, Delete)*
2. *SCM Config Change Policies Management (Query, Create, Modify, Delete, Execute)*
3. *SCM Default Communication Parameters Management (Modify)*
4. *SCM Device Configuration Files Management (Download, Upload, Query, Modify)*

6.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. *SolarWinds Web Console user:*
    a. *SolarWinds Administrator*
    b. *SolarWinds User*
2. *NCM user role for accessing NCM-specific data via the SolarWinds Web Console:*
    a. *Administrator*
    b. *Engineer*
    c. *Web Uploader*
    d. *WebDownloader*
    e. *WebViewer*
    f. *None*
3. *IPAM user role for accessing IPAM-specific data via the SolarWinds Web Console:*
    a. *Admin*

   b. *Power User*
   c. *Operator*
   d. *Read Only*
4. *EOC Web Console user:*
   a. *Administrator*
5. *Solarwinds Windows application user:*
   a. *Windows Application Administrator*
6. *SAM user role for accessing SAM-specific data via the SolarWinds Web Console:*
   a. *Administrator*
   b. *User*
7. *SCM user role for accessing SCM-specific data via the SolarWinds Web Console:*
   a. *Administrator*
   b. *User*

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: For EOC, the Administrator role is defined as any user with the Allow Administrator Rights permission.

6.1.4 Network Management (FNM)

6.1.4.1 FNM_MDC.1 Monitor Data Collection

FNM_MDC.1.1 The TSF shall be able to store configuration, status and performance information received via real-time feeds and/or polling.

6.1.4.2 FNM_ANL.1 Monitor Analysis

FNM_ANL.1.1 The TSF shall perform the following analysis function(s) on all status and performance information received from managed elements:

1. Status changes;
2. Threshold values exceeded;
3. Configuration changed; and
4. Configured conditions satisfied.

6.1.4.3 FNM_RCT.1 Management React

FNM_RCT.1.1 The TSF shall perform the specified alert notification action(s) when conditions regarding the status or performance of managed elements and specified by an administrator are detected.

Application Note: The TOE monitors a variety of status and performance indicators for managed elements; the specific items are dependent on the type of elements being monitored. Administrators may configure alerts to be generated

based on status changes of managed elements (e.g. node down) or performance threshold values being exceeded (e.g. CPU utilization of a server exceeds a threshold value).

6.1.4.4 FNM_RDR.1 Restricted Data Review

Application Note: Different Monitor data privileges are enforced for different TOE access mechanisms and categories of data. The first iteration applies to all Monitor data on a specific SolarWinds Server instance other than configuration files uploaded from monitored devices. The second iteration deals specific with device configuration files since access privileges are based on NCM roles and not all SolarWinds user accounts have an NCM role assigned. The third iteration specifies access from EOC, since individual EOC user accounts may be configured to have access to different subsets of SolarWinds servers.

6.1.4.4.1 FNM_RDR.1(1) Restricted Data Review (Authorized SolarWinds Web Console Users)

FNM_RDR.1.1(1) The TSF shall provide *authorized SolarWinds Web Console users* with the capability to read *Monitor data other than device configuration data* from the Monitor data.

FNM_RDR.1.2(1) The TSF shall provide the Monitor data in a manner suitable for the user to interpret the information.

FNM_RDR.1.3(1) The TSF shall prohibit all users read access to the Monitor data, except those users that have been granted explicit read-access.

6.1.4.4.2 FNM_RDR.1(2) Restricted Data Review (Authorized SolarWinds Web Console Users That Have NCM Roles Configured)

FNM_RDR.1.1(2) The TSF shall provide *authorized SolarWinds Web Console users that have NCM roles configured* with the capability to read *device configuration data* from the Monitor data.

FNM_RDR.1.2(2) The TSF shall provide the Monitor data in a manner suitable for the user to interpret the information.

FNM_RDR.1.3(2) The TSF shall prohibit all users read access to the Monitor data, except those users that have been granted explicit read-access.

6.1.4.4.3 FNM_RDR.1(3) Restricted Data Review (Authorized EOC Web Console Users)

FNM_RDR.1.1(3) The TSF shall provide *authorized EOC Web Console users* with the capability to read *Monitor data from SolarWinds Servers the user is authorized to access* from the Monitor data.

FNM_RDR.1.2(3) The TSF shall provide the Monitor data in a manner suitable for the user to interpret the information.

FNM_RDR.1.3(3) The TSF shall prohibit all users read access to the Monitor data, except those users that have been granted explicit read-access.

6.1.4.5 FNM_STG.1 Guarantee of Monitor Data Availability

FNM_STG.1.1 The TSF shall protect the stored Monitor data from unauthorised deletion via operations under the control of the TSF.

FNM_ STG.1.2 The TSF shall protect the stored Monitor data from modification via operations under the control of the TSF.

Application Note: Authorised deletion of data is not considered a modification of Monitor data in this context. This requirement applies to the actual content of the Monitor data, which should be protected from any modifications.

6.1.5 TOE Access (FTA)

6.1.5.1 FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a *configured inactivity time for SolarWinds Web Console users, unless the inactivity timer functionality is disabled for the user account*.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 and is augmented by ALC_FLR.2. These requirements are summarized in the following table.

Table 18 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 19 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by OE.TIME
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_ATD.1 (all iterations)	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_UID.2	FIA_UID.1	None	n/a
FIA_USB.1(1)	No other components.	FIA_ATD.1(1)	Satisfied
FIA_USB.1(2)	No other components.	FIA_ATD.1(2)	Satisfied
FIA_USB.1(3)	No other components.	FIA_ATD.1	Satisfied by OE.WINDOWSACCESS
FMT_MTD.1(1)	No other components.	FMT_SMF.1(1), FMT_SMR.1	Satisfied, Satisfied
FMT_MTD.1(2)	No other components.	FMT_SMF.1(2), FMT_SMR.1	Satisfied, Satisfied
FMT_MTD.1(3)	No other components.	FMT_SMF.1(3), FMT_SMR.1	Satisfied, Satisfied
FMT_MTD.1(4)	No other components.	FMT_SMF.1(4), FMT_SMR.1	Satisfied, Satisfied
FMT_MTD.1(5)	No other components.	FMT_SMF.1(5), FMT_SMR.1	Satisfied, Satisfied
FMT_MTD.1(6)	No other components.	FMT_SMF.1(6), FMT_SMR.1	Satisfied, Satisfied
FMT_SMF.1 (all iterations)	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
FNM_MDC.1	No other components.	None	n/a
FNM_ANL.1	No other components.	FNM_MDC.1	Satisfied
FNM_RCT.1	No other components.	FNM_ANL.1	Satisfied
FNM_RDR.1 (all iterations)	No other components.	FNM_MDC.1, FNM_ANL.1	Satisfied, Satisfied
FNM_STG.1	No other components.	FNM_MDC.1, FNM_ANL.1	Satisfied, Satisfied
FTA_SSL.3	No other components.	None	n/a

7. TOE Summary Specification

7.1 Security Functions

7.1.1 Audit

Relevant SFRs: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2

The TOE generates audits for the events specified in the table included with FAU_GEN.1. Startup and shutdown of the audit function is controlled by changes to the Enable Audit Trail

setting; the evaluated configuration requires this value to be set at all times. The following fields are included in all audit log records, although not all fields are populated in all records:

- Date/time
- Message (details of the event)
- User performing the action

Audit records are stored in plaintext in the SolarWinds database for the time period configured via the Audit Trails Retention parameter, and are automatically deleted when the retention period expires.

Audit records may be viewed via the SolarWinds Web Console using the Message Center View by SolarWinds Administrators. Users are not permitted to read audit records.

7.1.2 Identification and Authentication

Relevant SFRs: FIA_ATD.1(all iterations), FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1(all iterations), FTA_SSL.3, FIA_AFL.1

The TOE provides the following access mechanism for users to interact with the TOE:

1. SolarWinds Web Console
2. EOC Web Console
3. SolarWinds Windows applications invoked on servers hosting TOE components

The first two mechanisms are accessed via web browsers from remote IT systems, while the third is accessed by users from the local keyboard/display on the servers hosting the TOE components.

When a connection is established to the SolarWinds Web Console, the TOE collects a username and password from the user. A dot ("•") is echoed for each character supplied for the password (FIA_UAU.7). Once the credentials are supplied, they are validated by the TOE (FIA_UID.2, FIA_UAU.2). If the credentials are not valid, the user account is not enabled, or the user account has expired, an error message is displayed and the user may try again. When max attempts reached due to authentication failure, user account will be locked for certain time of period (default is 15 minutes, it's configurable). This function is achieved by providing counts on authentication failure (FIA_AFL.1). If the credentials are valid, the security attributes configured for the supplied username (FIA_ATD.1(1)) are bound to the session (FIA_USB.1(1)) and the user is given access to the management functions. The attributes bound to the session are specified in FIA_USB.1(1). Sessions are automatically terminated after the configured inactivity time (FTA_SSL.3).

When a connection is established to the EOC Web Console, the TOE collects a username and password from the user. A dot ("•") is echoed for each character supplied for the password (FIA_UAU.7). Once the credentials are supplied, they are passed to the host operating system (Windows) for validation. If the credentials are not valid, an error message is displayed and the user may try again. If the credentials are valid, the supplied username is checked against the user accounts defined for the EOC Web Console (FIA_UID.2). If the account is not defined, an error message is displayed and the user may try again. If the user account is defined, the security attributes configured for the supplied username (FIA_ATD.1(2)) are bound to the session

(FIA_USB.1(2)) and the user is given access to the management functions. The attributes bound to the session are specified in FIA_USB.1(2).

When the SolarWinds Server is invoked via a Windows application, the TOE does not perform any I&A function. The user is required to have been identified by Windows (per OE.WINDOWSACCESS). The role bound to all users of this access mechanism is set to the Windows Application Administrator role (FIA_USB.1(3)).

When a user of the EOC Web Console accesses data from an SolarWinds Server, credentials for the user are automatically sent to the server on behalf of the user. If the user account is configured to use the configured credentials, the credentials used are those configured for the user account. Otherwise, the user is prompted for the credentials to send. A dot ("•") is echoed for each character supplied for the password (FIA_UAU.7).

When a user of the EOC Web Console or SolarWinds Web Console accesses configuration data (related to NCM) for a Node, the NCM role configured for the SolarWinds Server user account is bound to the session.

7.1.3 Management

Relevant SFRs: FMT_MTD.1(all iterations), FMT_SMF.1, FMT_SMR.1

Management functionality is available to authorized users through the SolarWinds Web Console, the EOC Web Console, and Windows applications invoked on the SolarWinds Servers. The management functionality available to users is specified in FMT_SMF.1. The functionality made available to individual users is dependent on their security attributes (including role), which vary based upon the TOE access mechanism being used. The roles are specified in FMT_SMR.1, and the access privileges available and associated security attributes are specified in FMT_MTD.1.

7.1.4 Network Monitoring

Relevant SFRs: FNM_ANL.1, FNM_MDC.1, FNM_RCT.1, FNM_RDR.1(all iterations), FNM_STG.1

Network monitoring is performed against Managed Elements by SolarWinds Servers. The types of monitoring are dependent on the TOE components installed on the SolarWinds Servers, and may include nodes, interfaces, servers, applications, IP address space, network flows, and SLAs.

Performance monitoring is performed by sending ICMP and/or SNMP messages to the Managed Elements to determine configuration information and retrieve status and statistics information. Status information may also be determined from Syslog and/or SNMP Trap messages received from the Managed Elements, or via WMI exchanges to determine information about servers and applications. All the information can store in the TOE for analysis purpose (FNM_MDC.1).

Information collected from the managed elements is analyzed (FNM_ANL.1). The TOE analyzes for a variety of status and performance indicators for managed elements; the specific items are dependent on the type of elements being monitored. The results of the analysis are available to authorized SolarWinds Web Console users or authorized EOC Web Console users of the TOE via Views (FNM_RDR.1). Events are generated to record status changes or configured threshold values being met concerning the managed elements (FNM_ANL.1), and Alerts may be generated based upon these conditions being detected about the managed elements (FNM_RCT.1). SolarWinds Administrators may configure alerts to be generated based on status

changes of managed elements (e.g. node down) or performance threshold values being exceeded (e.g. CPU utilization of a server exceeds a threshold value). Alerts may cause notifications such as Syslog messages or SNMP Trap messages sent to configured destinations.

The results of the analysis are available to users of the TOE via Views (FNM_RDR.1). Views may be accessed via the SolarWinds Web Console, which provides information concerning Managed Elements configured in a specific SolarWinds Server instance; or the EOC Web Console, which provides aggregated information from one or more SolarWinds Server instances, depending on the configuration for individual EOC Web Console users.

Access privileges for status and analysis information maintained by the SolarWinds Server is determined by the user account privileges configured for each authorized SolarWinds n Server user account.

The information collected from the managed elements, as well as the analysis results, is saved in the TOE database and may be reviewed by authorized users (FNM_STG.1). The TOE does not provide any direct database access to SolarWinds Web Console or EOC Web Console users, and the mediated access does not provide any mechanism to modify the Monitor data. The only mechanism provided to delete Monitor data is via the configuration of data retention policies by authorized SolarWinds Administrators.

7.1.5 Configuration Management

Relevant SFRs: FMT_MTD.1(2), FNM_ANL.1, FNM_RCT.1

The TOE downloads configuration files from network nodes either on command by an authorized NCM user or according to scheduled NCM jobs (FMT_MTD.1(2)). Configuration files may also be uploaded to network nodes on command by an authorized NCM user or according to scheduled NCM jobs (FMT_MTD.1(2)).

When configuration files are downloaded, they may be compared to previously downloaded files to detect changes (FNM_ANL.1). Syslog messages received from the network nodes may also be analyzed to detect configuration changes (FNM_ANL.1). Detection of a configuration change can trigger the upload of a configuration file to a network node (FNM_RCT.1).

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat, assumption, and organisational security policy is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 20 - Threats, Assumptions, and Organisational Security Policies to Security Objectives Mapping

	O.AUDITS	O.AUDIT_REVIEW	O.CONFIG	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TOE_ACCESS	OE.COMM	OE.CRYPTO	OE.DBACCESS	OE.DBMONITOR	OE.ENVIRON	OE.INSTALL	OE.INTROP	OE.NETWORK	OE.NOEVILADMIN	OE.SSL	OE.TIME	OE.WINDOWSACCESS
A.ACCESS														X					
A.ASCOPE													X						
A.DBACCESS										X									
A.ENVIRON												X							
A.INSTALL													X						
A.NETWORK															X				
A.NOEVILADMIN																X			
P.ACCACT	X						X											X	
P.ACCESS				X			X												X
P.ANALYZ			X		X														
P.DBMONITOR											X								
P.DISCLOSURE								X	X								X		
P.INTGTY				X															
P.MANAGE							X												X
P.PASSWORDS						X													
T.INTERCEPT									X										
T.MASQUERADE							X	X											X
T.TSF_COMPROMISE				X															
T.UNIDENT_ACTIONS	X	X																X	

The following table describes the rationale for the threats, assumptions, and organisational security policies to security objectives mapping.

Table 21 - Threats, Assumptions and Organisational Security Policies to Security Objectives Rationale

TYPE	Security Objectives Rationale
A.ACCESS	The **OE.INTROP** objective ensures the TOE has the needed access.
A.ASCOPE	The **OE.INSTALL** objective ensures the TOE is installed per the vendor guidance, which addresses scalability.
A.DBACCESS	The **OE.DBACCESS** objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators according to guidance document, such that only authorized users may utilize the mechanisms.
A.ENVIRON	**OE.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.INSTALL	**OE.INSTALL** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NETWORK	**OE.NETWORK** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NOEVILADMIN	**OE.NOEVILADMIN** addresses this assumption by restating it as an objective for the Administrator to satisfy.
P.ACCACT	The **O.AUDITS** objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The **OE.TIME** objective supports this policy by providing a time stamp for insertion into the audit records. The **O.TOE_ACCESS** objective supports this objective by ensuring each user is identified and authenticated.
P.ACCESS	**O.MANAGE** defines the access privileges to the data for the supported roles. **O.TOE_ACCESS** requires the TOE to control access based upon the user's role. **OE.WINDOWSACCESS** requires Windows to restrict access to SolarWinds Server functionality via Windows applications to users authorized to invoke TOE functionality.
P.ANALYZ	**O.CONFIG** requires the TOE to be able to compare configuration files for managed elements to detect unexpected changes. **O.MONITOR** requires the TOE to analyze information collected from the managed elements to detect conditions specified by administrators.
P.DBMONITOR	**OE.DBMONITOR** addresses this policy by restating it as an objective for the Administrator to satisfy.
P.DISCLOSURE	**OE.COMM** addresses the policy by requiring the environment to supply functionality to protect the communication between remote systems and TOE components. **OE.CRYPTO** addresses the policy by requiring the environment to provide cryptographic functionality in support of data protection protocols such as SSL. **OE.SSL** addresses the policy by requiring the environment to provide SSL as a data protection protocol.
P.INTGTY	**O.MANAGE** requires the TOE to define the required functionality, which also implicitly defines the lack of functionality for modification of collected data.
P.MANAGE	**O.TOE_ACCESS** requires the TOE to control access based upon the user's role, which requires the TOE to bind a role to each user's session. **OE.WINDOWSACCESS** requires Windows to restrict access to SolarWinds Server functionality via Windows applications to users authorized to invoke TOE functionality.

TYPE	Security Objectives Rationale
P.PASSWORDS	**O.PASSWORDS** addresses this policy by requiring the TOE to provide functionality for Administrators, but not non-Administrators, to configure passwords.
T.INTERCEPT	**OE.CRYPTO** mitigates the threat by requiring the environment to provide cryptographic functionality in support of secure communication channels.
T.MASQUERADE	**O.TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. **OE.COMM** mitigates this threat by protecting data when it is transferred between remote systems and the TOE. **OE.WINDOWSACCESS** requires Windows to identify and authenticate users before they access SolarWinds Server functionality via Windows applications.
T.TSF_COMPROMISE	**O.MANAGE** is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data.
T.UNIDENT_ACTIONS	The **O.AUDITS** objective helps to mitigate this threat by recording actions for later review. The **O.AUDIT_REVIEW** objective helps to mitigate this threat by providing the Administrator with the ability to review the actions taken by administrators. The **OE.TIME** helps to mitigate this threat by ensuring that correct timestamps are available for audit records.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 22 - SFRs to Security Objectives Mapping

	O.AUDITS	O.AUDIT_REVIEW	O.CONFIG	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TOE_ACCESS
FAU_GEN.1	X						
FAU_SAR.1		X					
FAU_SAR.2		X					
FIA_AFL.1							X
FIA_ATD.1 (all iterations)				X			X
FIA_UAU.2							X
FIA_UAU.7							X

	O.AUDITS	O.AUDIT_REVIEW	O.CONFIG	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TOE_ACCESS
FIA_UID.2							X
FIA_USB.1 (all iterations)							X
FMT_MTD.1(1)				X		X	
FMT_MTD.1(2)			X	X			
FMT_MTD.1(3)				X			
FMT_MTD.1(4)				X			
FMT_MTD.1(5)				X			
FMT_MTD.1(6)				X			
FMT_SMF.1 (all iterations)				X			
FMT_SMR.1				X		X	
FNM_MDC.1			X		X		
FNM_ANL.1			X		X		
FNM_RCT.1					X		
FNM_RDR.1(1)				X	X		
FNM_RDR.1(2)			X	X	X		
FNM_RDR.1(3)				X	X		
FNM_STG.1			X		X		
FTA_SSL.3							X

The following table provides the detail of TOE security objective(s).

Table 23 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDITS	**FAU_GEN.1** requires the TOE to generate audit log records for a specified set of security-relevant events.
O.AUDIT_REVIEW	**FAU_SAR.1** requires the TOE to provide authorized users with a mechanism to review audit logs. **FAU_SAR.2** requires the TOE to prevent unauthorized users from reading the audit logs.
O.CONFIG	**FMT_MTD.1(2)** defines the roles that may perform configuration management operations with the managed elements. **FNM_ANL.1** requires the TOE be able to compare configuration files for managed elements. **FNM_MDC.1** requires the TOE be able to store collected configuration file. **FNM_RDR.1(2)** requires that configuration file be able to be viewed in human readable form by authorized user only. **FNM_STG.1** requires the TOE to protect configuration files from modification or unauthorized deletion.

Security Objective	SFR and Rationale
O.MANAGE	**FIA_ATD.1(all iterations)** define the security attributes that must be able to be managed for users of the TOE. **FMT_MTD.1(all iterations)** defines the data access privileges associated with each role. **FMT_SMF.1(all iterations)** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported. **FNM_RDR.1(all iterations)** requires the TOE to provide information collected from managed elements to be displayed in human readable form.
O.MONITOR	**FNM_MDC.1** requires the TOE be able to collect and save information about the managed elements **FNM_ANL.1** requires the TOE to be able to analyze the information collected about the managed elements. **FNM_RCT.1** requires the TOE be able to generate alerts upon detection of performance and status of the configured managed elements. **FNM_RDR.1(all iterations)** requires that data collected about the managed elements and analysis results be able to be viewed in human readable form. **FNM_STG.1** requires the TOE to protect configuration files from modification or unauthorized deletion.
O.PASSWORDS	**FMT_MTD.1(1)** defines the access privileges for Administrators and non-Administrators, stating that only Administrators may configure user accounts (password is one of the attributes). **FMT_SMR.1** defines the specific security roles to be supported.
O.TOE_ACCESS	**FIA_AFL.1** requires the TOE detect user login attempt and lock user account when the number of authentication failure reached the providing counts. **FIA_ATD.1(all iterations)** defines the attributes of users, including a username that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE (e.g., the TOE associates a username with a role). **FIA_UID.2** requires that a user be identified to the TOE in order to access TOE functionality or data. **FIA_UAU.2** requires that a user of the SolarWinds Web Console be authenticated by the TOE before accessing TOE functionality or data. **FIA_UAU.7** provides that the authentication data provided by the user is not echoed back in plaintext, thus serving to protect that data. **FIA_USB.1(all iterations)** defines the attributes that are bound to user sessions for the access mechanisms provided by the TOE. **FTA_SSL.3** requires the TOE to automatically terminate user sessions that are inactive, which protects against unauthorized users gaining access via a "forgotten" session.

8.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from part 3 of the Common Criteria.