SolarWinds ORION® Software Security Target

Version 1.8

March 23, 2012

SolarWinds Worldwide, LLC
3711 South MoPac Expressway
Building Two
Austin, Texas 78746

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

SolarWinds Worldwide, LLC
3711 South MoPac Expressway
Building Two
Austin, Texas 78746
http://www.solarwinds.com

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

APM ..... **ORION Application Performance Monitor™**
CC ..... **Common Criteria**
CIDR ..... **Classless Internet Domain Routing**
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**
HTTP ..... **HyperText Transfer Protocol**
HTTPS ..... **HTTP Secure**
ICMP ..... **Internet Control Message Protocol**
IMAP ..... **Internet Message Access Protocol**
IP ..... **Internet Protocol**
IPAM ..... **ORION IP Address Manager™**
IPSLA ..... **ORION IP SLA Manager™**
IT ..... **Information Technology**
MOS ..... **Mean Opinion Score**
NCM ..... **ORION Network Configuration Manager™**
NPM ..... **ORION Network Performance Monitor™**
NTA ..... **ORION NetFlow Traffic Analyzer™**
POP ..... **Post Office Protocol**
SCP ..... **Secure CoPy**
SFTP ..... **Secure FTP**
SLA ..... **Service Level Agreement**
SNMP ..... **Simple Network Management Protocol**
SSH ..... **Secure SHell**
SSL ..... **Secure Socket Layer**
ST ..... **Security Target**
TCP ..... **Transmission Control Protocol**
TOE ..... **Target of Evaluation**
ToS ..... **Type of Service**
TSF ..... **TOE Security Function**
UDP ..... **User Datagram Protocol**
URL ..... **Uniform Resource Locator**
VoIP ..... **Voice over IP**
WAN ..... **Wide Area Network**
WMI ..... **Windows Management Instrumentation**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the SOLARWINDS® ORION® software TOE. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*and all international interpretations through March 30, 2011. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

SolarWinds Orion Software Security Target, version 1.8, March 23, 2012.

1.2 TOE Reference

SolarWinds Orion Network Performance Monitor (NPM) V10.1.3, Orion Application Performance Monitor (APM) V4.0.0, Orion Network Configuration Manager (NCM) V6.1.0, Orion Netflow Traffic Analyzer (NTA) V3.7.0, Orion IP Address Manager (IPAM) V1.7.0, Orion IP SLA Manager (IPSLA) V3.5.0, and Orion Enterprise Operations Console (EOC) V1.3.0

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 Release 3.

1.4 Keywords

Performance Monitor, Configuration Manager, Performance Manager, NetFlow Traffic Analyzer, Address Manager, SLA, Service Level Agreement, SLA Manager

1.5 TOE Overview

1.5.1 Usage and Major Security Features

Orion is a set of applications executing on one or more Windows servers. The applications monitor a configured set of network 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.

The Orion family consists of the following network, application, system, and storage monitoring and management products:

Orion Network Performance Monitor - Orion Network Performance Monitor (Orion 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.

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

Orion Network Configuration Manager - Orion Network Configuration Manager (Orion NCM) notifies network managers in real-time when device configurations change, helping network managers determine which changes could potentially cause network issues. Orion NCM

also provides nightly configuration backups, bulk configuration changes, user tracking, and inventory and compliance reporting.

Orion NetFlow Traffic Analyzer - Orion NetFlow Traffic Analyzer (Orion 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. Orion NTA provides a comprehensive view of the network traffic, enabling network managers to find the bottlenecks or identify the bandwidth hogs.

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

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

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

The Orion product suite 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 other SNMP-enabled devices to ensure peak network performance.
- 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.
- 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.
- 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.
- Create a custom poller to monitor any SNMP-enabled device, collect detailed data from MIB tables, & monitor virtually any statistic available on network devices. This functionality is not evaluated.
- Install additional polling engines for large networks with a small number of NPM or APM instances. This functionality is not evaluated.
- Install additional web servers to support a large number of network managers. This functionality is not evaluated.

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 Orion Servers are deployed. The Orion Web Console provides access to individual Orion Servers. The NCM Web Console provides access to detailed information provided by Orion NCM. 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 Orion Web Console interface, and by Windows for the EOC Web Console and NCM Web Console interfaces. 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.

Orion Servers also provide user interfaces for configuration of specific parameters within the TOE via Windows application programs. These tasks are performed by invoking applications via the Windows Start menu. For the applications to configure NCM, users are required to provide valid credentials before performing any other action. For the other Windows applications providing TOE access, any user with access to these applications must first authenticate to Windows and is then assumed to be authorized to perform the configuration actions.

1.5.2 TOE type

Network Management

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. Orion Server - NPM and/or APM installed on a dedicated server. Any combination of NCM and/or Orion modules (NTA, IPAM and/or IPSLA) may also be installed with each instance. Any combination is generically referred to as an Orion Server.

Table 1 - EOC Server Minimum Hardware and Software Requirements

Item	Requirements
Operating System	32-bit or 64-bit Microsoft Windows Server 2003 or Windows Server 2008 (including R2)
Web Server	Internet Information Service 6.0 or later
.NET Framework	Version 3.5 or later
CPU	3.0 GHz
Memory	2 GB
Available Disk Space	100 MB
DBMS	Microsoft SQL Server 2005 or SQL Server 2008. Express, Standard, or Enterprise

Table 2 - Orion Server Minimum Software Requirements

Item	Requirements
Operating System	Windows Server 2003 or 2008, including R2
Web Server	Microsoft IIS, version 6.0 and higher, in 32-bit mode
.NET Framework	Version 3.5 SP1 or later ASP .NET 2.0 Ajax Extension, Version 1 or later
SNMP Trap Services	Windows operating system management and monitoring tools
Web Browser	Microsoft Internet Explorer version 6 or higher with Active scripting, or Firefox 3.0 or higher

The hardware requirements for Orion Servers are dependent on the number of elements to be monitored and/or managed by the server.

Table 3 - Orion Server Minimum Hardware Requirements

Item	Requirements		
	<500 Elements	<2000 Elements	2000+ Elements
CPU	2.0 GHz	2.4 GHz	3.0 GHz
Memory	3 GB	4 GB	4 GB
Available Disk Space	2 GB	5 GB	20 GB

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

Table 4 - Database Server Minimum Software Requirements

Item	Requirements
DBMS	SQL Server 2005 SP1 Express, Standard, or Enterprise; or SQL Server 2008 Standard, or Enterprise
Operating System	Any Windows OS satisfying the minimum requirements for the DBMS
Additional Software	SQL Server System Common Language Runtime (CLR) Types Microsoft SQL Server Native Client Microsoft SQL Server Management Objects

The hardware requirements for Database Servers are dependent on the number of elements to be monitored and/or managed by the associated Orion Server.

Table 5 - Database Server Minimum Hardware Requirements

Item	Requirements		
	<500 Elements	<2000 Elements	2000+ Elements
CPU	2.0 GHz	2.4 GHz	3.0 GHz
Memory	2 GB	3 GB	4 GB
Available Disk Space	2 GB	5 GB	20 GB

Credential validation for the EOC Web Console and NCM Web Console interfaces 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 Orion Server 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.

When connecting to network devices, the TOE supports the use of SSH as well as Telnet. Files transferred from the network devices to the TOE may use SFTP or SCP. The SSL functionality used for these operations is provided by the operational environment.

1.6 TOE Description

The Orion software 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 or applications that can be monitored by standard mechanisms such as SNMP, ICMP, Syslog or WMI. NCM 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.

Users interact with the TOE via multiple mechanisms. Web Consoles are provided for remote interaction with the EOC, NPM, APM, and NCM functionality (as well as any modules added to NPM/APM). Application programs to configure the TOE may also be invoked from the Windows Start menu by authorized users.

1.6.1 Physical Boundary

The TOE consists of the SolarWinds Orion software identified in section 1.2 executing on multiple dedicated Windows servers. The operating systems (including the network protocol stacks and cryptographic functionality), web servers and DBMS are outside the TOE boundary.

On an Orion Server, the physical boundary of the TOE includes the following Windows services that are part of the NPM and APM components:

1. SolarWinds Alerting Engine
2. SolarWinds Collector Data Processor
3. SolarWinds Collector Management Agent
4. SolarWinds Collector Polling Controller
5. SolarWinds Information Service
6. SolarWinds Job Engine
7. SolarWinds Job Engine v2
8. SolarWinds Job Scheduler
9. SolarWinds Orion Information Service v1
10. SolarWinds Orion Module Engine
11. SolarWinds Syslog Service
12. SolarWinds Trap Service

If NCM is installed on an Orion Server, the physical boundary of the TOE includes the NCM Integration Module as well as the following Windows services that are part of the NCM component:

1. SolarWinds Orion NCM Caching Service
2. SolarWinds Orion NCM Information Service
3. SolarWinds Orion NCM Polling Service
4. SolarWinds SFTP/SCP Server

The SolarWinds ToolSet distributed as part of the Orion product suite is not installed in the evaluated configuration and is not included in the physical boundary. All other parts of the Orion product suite distributed with the standard distribution mechanisms are included in the TOE boundary.

The physical boundary includes the following guidance documentation:

1. *SolarWinds® Orion® Common Components Administrator Guide*
2. *SolarWinds® Orion® Network Performance Monitor Administrator Guide*
3. *SolarWinds® Orion® Application Performance Monitor Administrator Guide*
4. *SolarWinds® Orion® Enterprise Operations Console Administrator Guide*
5. *SolarWinds® Orion® IP SLA Manager Administrator Guide*

6. *SolarWinds® Orion® NetFlow Traffic Analyzer Administrator Guide*
7. *SolarWinds® Orion® IP Address Manager Administrator Guide*
8. *SolarWinds® Orion® Common Criteria Supplement*

1.6.2 Logical Boundary

The TOE provides the following security functionality:

1. Identification and Authentication – When a connection is established to any of the Web Consoles, the TOE prompts the user for login credentials. The credentials are validated by the TOE for the Orion Server Web Console. For the EOC and NCM Web Consoles, the credentials are first passed to Windows for validation. For Windows application providing configuration capabilities for NCM, the TOE prompts the user for login credentials. If the credentials are valid, the username is used to retrieve the user's security attributes inside the TOE from the TOE database.
2. Management – Management functionality is provided to authorized users. The functionality provided to individual users is determined by the user's role, which is one of the security attributes for users.
3. 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 in respond to configured conditions detected about the managed elements.
4. 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.

The following functionality included in the Orion product suite is not evaluated:

- Create a custom poller to monitor any SNMP-enabled device, collect detailed data from MIB tables, & monitor virtually any statistic available on network devices.
- Install additional polling engines for large networks with a small number of NPM or APM instances.
- Install additional web servers to support a large number of network managers.
- External web sites are not added to Orion Server Web Console views.
- The "Check for product updates" function is not used.
- Custom device pollers are not configured. Pollers supplied with the TOE are included in the evaluation.
- Custom component monitors are not configured. Component monitors supplied with the TOE are included in the evaluation. Account limitations are tied to custom component monitors and are also not configured.
- Custom property functionality is not configured. Built-in properties are included in the evaluation.

- Advanced Alerts (which use custom properties) are not configured. Basic Alerts are included in the evaluation.
- Orion Server failover functionality is not configured.
- The functionality to remotely manage interfaces in Network Devices.
- Custom NCM device templates are not configured. The default device templates supplied with the TOE are included in the evaluation.
- Customized views are not configured on Orion Server Web Consoles; default Views are used (the Allow Account to Customize Views permission may be set to allow specification of credentials for the NCM Integration Module).
- View Limitations are not configured.
- Customized page views are not configured on EOC Server Web Consoles; default page views are used (the Allow User To Personalize Their Pages permission is not set).

1.6.3 TSF Data

The following table describes the TSF data.

Table 6 - TSF Data Descriptions

TSF Data	Description
Data Related to Orion Servers or Orion Server 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 • Monitored property • Monitored objects • Trigger and reset conditions • Time of day • Suppression parameters • 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.
APM Settings	Configured information used for monitoring applications. The information includes: • Credential sets • Polling parameters • Data retention policies
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.

TSF Data	Description
Assigned Component Monitors	Define the assignment of application monitor templates to Network Devices hosting an application to be monitored.
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.
IP SLA CallManager Nodes	Define the set of Cisco CallManager and CallManager Express devices to be monitored by the IP SLA functionality.
IP SLA Operations	Define test measurements to be performed by the IP SLA functionality on IP SLA 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 • IP SLA Nodes • Warning threshold • Critical threshold
IP SLA Settings	Define the operation of IP SLA 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
IP SLA VoIP Nodes	Define the set of VoIP devices that are monitored by the IP SLA functionality.
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
IPAM DHCP Scopes	Define the DHCP scopes configured in Cisco IOS and Microsoft DHCP servers that are monitored by the IPAM functionality. Parameters include: • DHCP Server • Scan parameters

TSF Data	Description
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 Integration Module Configurations	Define the connection parameters for an Orion Server instance to interact with a co-located NCM Server. Parameters include: • IP address of the NCM Server
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 IP SLA
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 Web Console.
Reports	Pre-defined Reports may be viewed via the Web Console.
SNMP Credential Sets	Define credentials used to communicate with Network Devices via SNMP to obtain information.
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.

TSF Data	Description
Thresholds	Define values for devices that cause warning or error indicators to be displayed in the Web Console. Threshold values may be set for: • CPU Load • Disk Usage • Percent Memory Used • Percent Packet Loss • Response Time • Availability • Node Warning Interval
Traps	The set of SNMP trap messages that have been received from Network Devices.
User Accounts	Define the user accounts attributes for users authorized to access Orion Servers via the Web Console. Attributes include: • Username • Password • Enabled • Expiration Date • Disable Session Timeout • Allow Administrator Rights (Role) • Allow Node Management Rights • Allow Account to Customize Views • Allow Account to Clear Events and Acknowledge Alerts • Alert Sound • Views (restricts access to Views) • Report Folder (restricts access to Reports) • Menu Bar Assignments (limits access to specific GUIs) • Credentials used to access the NCM server data via the NCM Integration Module
Views	Define the views that may be invoked by users. Attributes include: • Resources included in the View
Web Console Settings	Defines parameters controlling the behavior of a Web Console session. Settings include: • Session Timeout • Page Refresh Time • Status Rollup Mode
Data Related to NCM or NCM Web Consoles	
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
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
Default NCM Alert	Defines the actions performed for the "Default NCM Alert" that is automatically generated for Alert processing on an Orion Server when NCM is installed.
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.
Groups	Define related Nodes.
Ignore List	Specifies a set of entities that are not added as Managed Devices even if they are found during discovery processes.
Inventory Settings	Specify the statistics collected from Nodes during Inventory Jobs.
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 • Email Notification Parameters • Syslog Receiver Parameters • SNMP Trap Receiver Parameters
Nodes	Defines the set of network devices managed by the TOE. The device types that may be managed include switches, routers, firewalls, and Windows servers. Attributes for each Node include: • Hostname or IP Address • SNMP Version • SNMP Parameters • Login Type (Device or User) • Device Login Credentials • Management Status (Managed or Unmanaged) • Communication Protocols and Ports
Reports	Define reports available for summarizing information known about the Nodes. Parameters include: • Name • Title • Description • Category • Nodes included • Information included • Filters

TSF Data	Description
SNMP Trap Server Settings	Configuration for the SNMP Trap receiver. Parameters include: • Trap retention period • Filters • Alerts
Syslog Server Settings	Configuration for the Syslog receiver. Parameters include: • Syslog message retention period • Filters • Alerts
User Accounts	Define the user account attributes for users authorized to access NCM. Attributes include: • Username • Role (Administrator, Engineer, WebDownloader, WebUploader, or WebViewer) • Device Login Credentials • Device Enable Level and Password
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 Orion Servers • Orion Server Credentials user-supplied or admin-supplied • Orion Server credentials
Menu Bars	Define a set of Views available to a role.
Orion Servers	Define the Orion Servers associated with the EOC. Attributes include: • Name • Hostname or IP Address • URL • Orion Server credentials • Polling interval • Enabled or disabled
Roles	Define the Views members assigned the role may access. Parameters include: • Name • Menu Bar

1.7 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 Orion Server, each installed on a dedicated Windows server. Each Orion Server has one or both of NPM and APM installed. Each Orion Server may have any combination of NCM, NTA, IPAM and/or IPSLA installed. If NCM is installed, the Orion Server integration module is also installed.
3. For each instance of the Orion 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. The SolarWinds Toolset optional component is not installed.
3. For any functions that can be performed both via the Web Consoles (Orion Server or NCM Server) and via Windows applications (invoked via the Start menu using the directly attached display/keyboard of the server hosting the Orion Server), guidance documentation directs the administrator to use the Web Console only to perform those functions.
4. Access to the Windows applications to invoke the TOE is restricted in Windows to users authorized to perform those functions, in particular: backup and restore the database, manage TOE Alerts, manage NCM user account attributes, and manage Report configuration settings.
5. The Customize option is not configured for any menu bars for the Orion Server Web Consoles.
6. External web sites are not added to Orion Server Web Console views.
7. The "Check for product updates" function is disabled. Installing product updates may update the product to a version that has not been evaluated.
8. Custom device pollers are not configured or evaluated. Pollers supplied with the TOE are included in the evaluation.
9. Custom component monitors are not configured or evaluated. Component monitors supplied with the TOE are included in the evaluation.
10. Custom property functionality is not configured or evaluated. Built-in properties are included in the evaluation and may be used to configure View limitations.
11. Advanced Alerts are not configured or evaluated. Basic Alerts are included in the evaluation.
12. Customized Views are not configured on Orion Server Web Consoles.
13. View Limitations are not configured.
14. Orion Server failover functionality is not configured or evaluated.
15. The functionality to remotely manage interfaces in Network Devices is not evaluated.
16. The IPAM role is configured as Default for all users, allowing the Orion Server role to determine the user access to IPAM functions.
17. The NTA Database Maintenance option is enabled in order to have the TOE automatically compress and purge data according to the configured periods.
18. When importing User Accounts into the TOE, only individual accounts are imported. Windows Group Accounts are not imported.
19. Only Administrators assign passwords for User Accounts defined in the TOE. Non-Administrators are not permitted to change their own passwords.

20. The Orion Server Browser Integration parameter is not enabled for User Accounts, since the operations performed via this integration are outside the control of the TOE.
21. The Allow User To Personalize Their Pages permission is not set for any EOC user accounts. Therefore, only the default page views are included in the evaluation.
22. Network Devices are imported into NCM from the co-located Orion Server.
23. The NCM "Require a login to use Orion Network Configuration Manager" parameter is set.
24. Built-in NCM user accounts are used during installation only. In operation, only standard user accounts are used.
25. Custom NCM device templates are not configured or evaluated. The default device templates supplied with the TOE are included in the evaluation.
26. Custom Configuration Change Templates are not configured or evaluated. The default configuration change templates supplied with the TOE are included in the evaluation.
27. The NCM Integration Module provides access to NCM-related information for Orion Server Web Service users The credentials used must be chosen by administrators to provide the lowest privileges appropriate for each of the users with access to this mechanism.
28. Real-time config change notification is not enabled in NCM since it is dependent on additional software beyond the scope of the evaluated products.
29. Per-device credentials are used rather than per-user device credentials.
30. All users of the NCM Integration Module must be configured to have the Allow Account to Customize Views permission (in order to enter their credentials for NCM access).
31. Because of inherent security limitations in TFTP, the TFTP server is never enabled on the Orion Server or EOC Server.

1.8 Rationale for Non-Bypassability and Separation

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied OSs.

Non-bypassability

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. All systems on which the TOE executes are dedicated systems.

Non-interference

The TOE is implemented with well defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security

relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple administrators by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components uses HTTPS to protect the information exchanged. The secure channels rely upon cryptographic functionality provided by the OS or third party software.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 3, dated July 2009

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 conformant.

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

2.3 Protection Profile Conformance

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

3. Security Problem Definition

3.1 Introduction

This chapter 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 policies as P.*policy*.

3.2 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 7 - 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.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary 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.

3.3 Threats

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

Table 8 - Threats

T.Type	Description
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data to be modified.

3.4 Organisational Security Policies

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

Table 9 - Organizational Security Policies

P.Type	Organizational Security Policy
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 distributed TOE components and between the TOE and remote users will be protected from disclosure.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
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.

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 10 - Security Objectives for the TOE

O.Type	Description
O.CHANNEL	The TOE will use trusted channels when sending credentials to Managed Elements to protect the credentials from disclosure.
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.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
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.

4.2 Security Objectives for the Operational Environment

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

Table 11 - Security Objectives of the Operational Environment

OE.Type	Description
OE.COMM	The Operational Environment will protect communication between distributed components of the TOE from disclosure.
OE.CRYPTO	The Operational Environment will provide cryptographic functionality needed to provide confidentiality with the protocols used for communication with remote IT Systems.
OE.DATABASE	Those responsible for the TOE must ensure that access to the TOE database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.
OE.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.

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 Administrator will 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. The 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.
OE.SSL	The Operational Environment will require incoming connections to the Web Services to use SSL/TLS.
OE.WINDOWSACCESS	Users invoking the Orion Server functionality via Windows application programs must successfully perform identification and authentication functions with Windows first, and access to the applications that invoke ORION Server functionality must be limited to users authorized to invoke TOE management functionality.

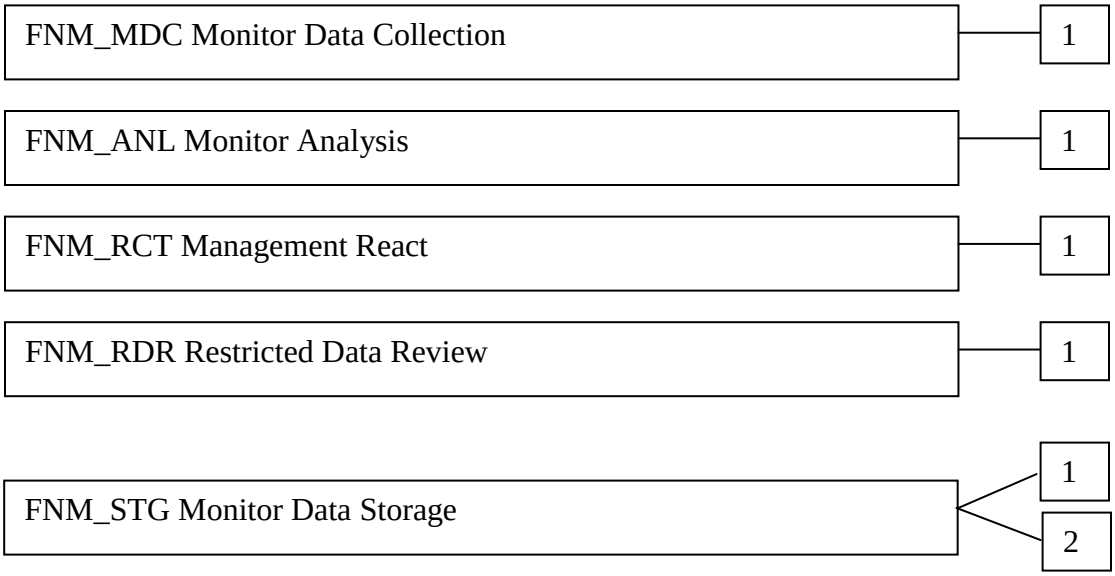
5. Extended Components Definition

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 Analyzer 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.

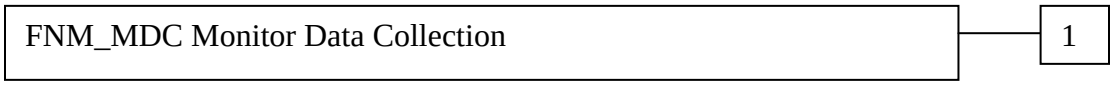


5.1.1.1 FNM_MDC Monitor Data Collection

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

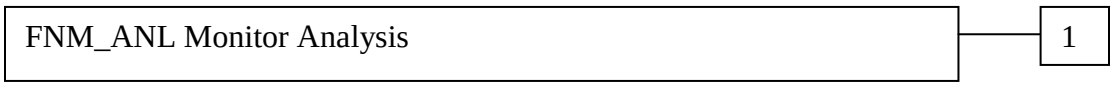
FNM_MDC.1.1 The TSF shall be able to store configuration, status and performance information received via real-time feeds and/or polling.

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.1 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

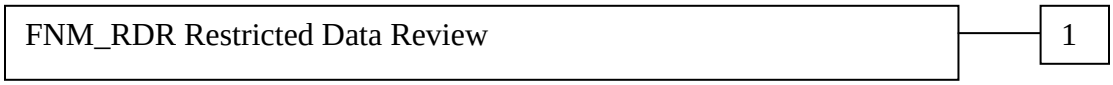
FNM_RCT.1.1 The TSF shall perform the configured alert action(s) when conditions specified by an administrator are detected.

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.

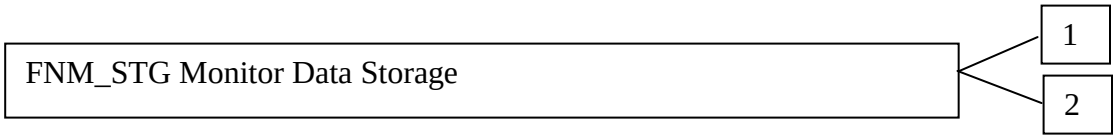
FNM_RDR.1.3 The TSF shall prohibit all users read access to the Monitor data, except those users that have been granted explicit read-access.

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.

FNM_STG.2 Prevention of Monitor Data Loss defines the actions to be taken if the monitor data storage capacity has been reached.

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.

Management: FNM_STG.2

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

a) maintenance (deletion, modification, addition) of actions to be taken in case monitor data storage capacity has been reached.

Audit: FNM_STG.1

There are no auditable events foreseen.

Audit: FNM_STG.2

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

a) Basic: Actions taken if the storage capacity has been reached.

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 within the TSC.

FNM_ STG.1.2 The TSF shall protect the stored Monitor data from modification within the TSC.

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.

FNM_STG.2 Prevention of Monitor data loss

Hierarchical to: No other components.

Dependencies: FNM_MDC.1 Monitor Data Collection

FNM_ANL.1 Monitor Analysis

FNM_STG.2.1 The TSF shall [selection: *'ignore Monitor data', 'prevent Monitor data, except those taken by the authorised user with special rights', 'overwrite the oldest stored Monitor data'*] if the storage capacity has been reached.

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 Identification and Authentication (FIA)

6.1.1.1 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 Orion 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.

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

1. *Username*
2. *Password*
3. *Account expiration date*
4. *Disable session timeout*
5. *Allow administrator rights (role)*
6. *Allow account to customize Views*
7. *Allow account to clear Events, acknowledge Alerts and Syslogs*
8. *Alert sound*
9. *Menu Bar assignments*
10. *Report folder*
11. *Credentials used to access the NCM server data via the NCM Integration Module*

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

FIA_ATD.1.1(2) The TSF shall maintain the following list of security attributes belonging to individual users **of the NCM Web Service and NCM Windows applications**:

1. *Username*
2. *Role*

Application Note: Different security attributes are maintained for different TOE access mechanisms. This iteration applies to security attributes for users of the NCM Web Service and NCM Windows applications.

FIA_ATD.1.1(3) The TSF shall maintain the following list of security attributes belonging to individual users **of the EOC Web Service**:

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

6.1.1.2 FIA_UAU.2 User Authentication Before any Action

Refinement Rationale: This SFR applies to password validation for the Orion Server Web Service. Password validation for the EOC and NCM Web Services and NCM Windows applications 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 **Orion Server Web Service** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.1.3 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.

6.1.1.4 FIA_UID.2 User Identification Before any Action

Refinement Rationale: This SFR applies to users accessing the TOE via the Orion Server Web Service, the NCM Web Service, NCM Windows applications or the EOC Web Service. The TOE does not perform any identification for users accessing the TOE via Orion Windows applications on servers on which Orion 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 **Orion Server Web Service, NCM Web Service, NCM Windows application and EOC Web Service** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.1.5 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.

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

1. *Username*
2. *Disable session timeout*
3. *Allow administrator rights (role)*
4. *Allow node management rights*
5. *Allow account to customize Views*
6. *Allow account to clear Events, acknowledge Alerts and Syslogs*
7. *Alert sound*
8. *Menu Bar assignments*
9. *Report folder*
10. *Credentials used to access the NCM server data via the NCM Integration Module*

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 **Orion Server Web Service** 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 **Orion Server Web Service** users: *User permissions (e.g. Allow administrator rights) 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; credentials used to access the NCM server data via the NCM Integration Module may be modified if the user account has the Allow Account to Customize Views permission; 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 Orion Server Web Service.

FIA_USB.1.1(2) The TSF shall associate the following user security attributes with subjects acting on behalf of that **NCM Web Service or NCM Windows application** user:

1. *Username*
2. *Role*

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 **NCM Web Service or NCM Windows application** 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 **NCM Web Service or NCM Windows application** 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 NCM Web Service and NCM Windows applications.

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

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

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 **EOC Web Service** users: *attributes are bound from the configured parameters for the identified user account*.

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 **EOC Web Service** 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 Service.

FIA_USB.1.1(4) The TSF shall associate the following user security attributes with subjects acting on behalf of that **Orion Windows applications** user:

1. *Role (Windows Application Administrator)*

FIA_USB.1.2(4) The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **Orion Windows applications** users: *the role is implied by use of the access mechanism*.

FIA_USB.1.3(4) The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **Orion 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 **Orion** Windows applications.*

6.1.2 Security Management (FMT)

6.1.2.1 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.

FMT_MTD.1.1(1) The TSF shall restrict the ability to query, modify, delete, clear, *create*, *acknowledge* the *Orion 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 Orion Servers.

Application Note: Orion Administrators are authorized Orion Server Web Service user accounts with the Allow Administrator Rights parameter value set.

Table 12 - Orion Server TSF Data Detail

TSF Data	Windows Application Administrator	Orion Administrator	Orion 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
APM Settings	None	Query and Modify	None
Application Monitor Templates	None	Query and Modify	None
Assigned Application Monitors	None	Query and Modify	None
Assigned Component Monitors	None	Query and Modify	None
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
Ignore List	None	Query Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set	Query
IP SLA CallManager Nodes	None	Query. Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	Query.

TSF Data	Windows Application Administrator	Orion Administrator	Orion User
IP SLA Operations	None	Query Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	Query
IP SLA Settings	None	Query Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	None
IP SLA VoIP Nodes	None	Query. Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	Query.
IPAM Addresses and Subnets	None	Query Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	Query
IPAM DHCP Scopes	None	Query Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	Query
IPAM Settings	None	Query Create, Modify and Delete if the "Allow Administrator Rights" account parameter is set	None
NCM Integration Module Configurations	None	Query and 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	None	None
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
SNMP Credential Sets	None	Query Create, Modify and Delete if the "Allow Node Management Rights" account parameter is set	Query

TSF Data	Windows Application Administrator	Orion Administrator	Orion User
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
User Accounts	None	Query, Create, Modify and Delete	None Modify their own credentials used to access the NCM server data via the NCM Integration Module if the "Allow Account to Customize Views" account parameter is set
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
Web Console Settings	None	Query and Modify	None

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, *create*, *execute*, *and schedule* the *NCM 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 NCM Servers.

Table 13 - NCM Server TSF Data Detail

TSF Data	Administrator	Engineer	Web Downloader	Web Uploader	Web Viewer
Config Change Templates	Query, Create, Modify, Delete, and Execute	Query, Create, Modify, Delete, and Execute	None	Query, Create, Modify, Delete, and Execute	None
Default Communication Parameters	Modify	None	None	None	None
Default NCM Alert	Modify	Modify	None	None	None
Device Configuration Files	Download, Upload, Query, Modify	Download, Upload, Query, Modify	Download, Query	Download, Upload, Query, Modify	Query

TSF Data	Administrator	Engineer	Web Downloader	Web Uploader	Web Viewer
Groups	Query, Create, Modify, and Delete	Query, Create, Modify, and Delete	Query	Query	Query
Inventory Settings	Modify	Modify	None	None	None
Jobs	Query and Create	Query and Create	None	None	None
NCM Settings	Modify	Modify	None	None	None
Nodes	Modify	Modify	Query	Query	Query
Reports	Query, Create, Modify, Delete, and Schedule	Query, Create, Modify, Delete, and Schedule	None	None	None
SNMP Trap Server Settings	Modify	None	None	None	None
Syslog Server Settings	Modify	None	None	None	None
User Accounts	Query, Create, Modify, and Delete	None	None	None	None

FMT_MTD.1.1(3) 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 14 - EOC Server TSF Data Detail

TSF Data	Administrator	Non-Administrator
EOC User Accounts	Query, Create, Modify, and Delete	None
Menu Bars	Query, Create, Modify, Delete, and Access	Access
Orion Servers	Query, Create, Modify, Delete, and Access	Access
Roles	Query, Create, Modify, and Delete	None

6.1.2.2 FMT_SMF.1 Specification of Management Functions

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

1. *User Account management*
2. *TOE settings management*
3. *Managed Element management*
4. *Alert management*

5. *Alert, Event, Syslog, and Trap review*
6. *Device configuration management*.

6.1.2.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. *Orion Server Web Services user:*
    a. *Orion Administrator*
    b. *Orion User*
2. *NCM Web Services or NCM Windows application user:*
    a. *Administrator*
    b. *Engineer*
    c. *Web Downloader*
    d. *Web Uploader*
    e. *Web Viewer*
3. *EOC Web Services user:*
    a. *Administrator*
    b. *Guest*
    c. *Other roles created by an Administrator*
4. *Orion Windows application user:*
    a. *Windows Application Administrator.*

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

6.1.3 Network Management (FNM)

6.1.3.1 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.

6.1.3.2 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.

6.1.3.3 FNM_RCT.1 Management React

FNM_RCT.1.1 The TSF shall perform the specified alert action(s) when conditions specified by an administrator are detected.

6.1.3.4 FNM_RDR.1Restricted Data Review

FNM_RDR.1.1(1) The TSF shall provide *authorized Orion Web Service users* with the capability to read *Monitor 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.

FNM_RDR.1.1(2) The TSF shall provide *authorized NCM Web Service users* with the capability to read *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.

FNM_RDR.1.1(3) The TSF shall provide *authorized EOC Web Service users* with the capability to read *Monitor data from Orion 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.

6.1.3.5 FNM_STG.1 Guarantee of Monitor Data Availability

FNM_STG.1.1 The TSF shall protect the stored Monitor data from unauthorised deletion within the TSC.

FNM_ STG.1.2 The TSF shall protect the stored Monitor data from modification within the TSC.

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.

6.1.3.6 FNM_STG.2 Prevention of Monitor Data Loss

FNM_STG.2.1 The TSF shall ignore Monitor data if the storage capacity has been reached.

6.1.4 TOE Access (FTA)

6.1.4.1 FTA_SSL.3 TSF-Initiated Termination

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

6.1.5 Trusted Path/Channels (FTP)

6.1.5.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF, another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *uploading configuration files, executing commands and scripts on the Managed Elements, polling managed elements using WMI.*

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in the following table.

Table 15 - EAL2 Assurance Requirements

Assurance Class	Component ID	Component Title
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
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 16 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FIA_ATD.1	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	No other components.	FIA_ATD.1	Satisfied

SFR	Hierarchical To	Dependency	Rationale
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied, Satisfied
FMT_SMF.1	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	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
FNM_STG.2	No other components.	FNM_MDC.1, FNM_ANL.1	Satisfied, Satisfied
FTA_SSL.3	No other components.	None	n/a
FTP_ITC.1	No other components.	None	n/a

7. TOE Summary Specification

7.1 Security Functions

7.1.1 Identification and Authentication

Relevant SFRs: FIA_ATD.1(*), FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1(*), FTA_SSL.3, FTP_ITC.1

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

1. Orion Server Web Service
2. NCM Web Service
3. EOC Web Service
4. Orion Windows applications invoked on servers hosting TOE components
5. NCM Windows applications

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

When a connection is established to the Orion Server Web Service, 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. If the credentials are valid, the security attributes configured for the supplied username (FIA_ATD.1) are bound to the session (FIA_USB.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, unless the timeout mechanism is disabled for the user account (FTA_SSL.3).

When a connection is established to the NCM Web Service or an NCM Windows application is invoked, 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 NCM (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) are bound to the session (FIA_USB.1) and the user is given access to the management functions. The attributes bound to the session are specified in FIA_USB.1(2).

When a connection is established to the EOC Web Service, 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 web service (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) are bound to the session (FIA_USB.1) and the user is given access to the management functions. The attributes bound to the session are specified in FIA_USB.1(3).

When the Orion 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).

When a user of the EOC Web Service accesses data from an Orion 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). Connections from the EOC Server to the Orion Servers (FTP_ITC.1) use SSL functionality (provided by the operational environment per OE.SSL) to protect the credentials from disclosure.

When a user of the EOC Web Service or Orion Server Web Service accesses configuration data (related to NCM) for a Managed Element, the NCM user account credentials configured for the Orion Server user account are transparently provided to the NCM Server on behalf of the EOC Web Service or Orion Server Web Service user. If no NCM credentials have been configured, the TOE collects a username and password from the user if the Orion user account has the Allow Account to Customize Views permission. 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 NCM (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) are bound to the session (FIA_USB.1) and the user is given access to the management functions. The attributes bound to the session are specified in FIA_USB.1(2). If the Orion user account does not have the Allow Account to Customize Views permission, the user may not specify NCM credentials and therefore may not access NCM via the integration module.

7.1.2 Management

Relevant SFRs: FMT_MTD.1(*), FMT_SMF.1, FMT_SMR.1

Management functionality is available to authorized users through the Orion Server Web Service, the NCM Web Service, the EOC Web Service, and Windows applications invoked on the Orion Servers. The management functionality available to users is specified in FMT_SMF.1. The functionality made available to individual users is dependent on their roles, which vary based upon the TOE access mechanism being used. The roles are specified in FMT_SMR.1, and the functionality available to each role is specified in FMT_MTD.1(*).

7.1.3 Network Monitoring

Relevant SFRs: FNM_ANL.1, FNM_MDC.1, FNM_RCT.1, FNM_RDR.1(*), FNM_STG.1, FNM_STG.2, FTP_ITC.1

Network monitoring is performed against Managed Elements by Orion Servers. The types of monitoring is dependent on the TOE modules installed on the Orion 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 (FNM_MDC.1). 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. Connections from the Orion Servers to the Managed Elements to upload configuration files, execute scripts or retrieve information via WMI (FTP_ITC.1) use SSL functionality (provided by the operational environment per OE.SSL) to protect the information (including credentials) from disclosure, using cryptographic functionality (provided by the operational environment per OE.CRYPTO). Syslog information sent by the managed elements to the TOE may be protected via SSL (FTP_ITC.1), using cryptographic functionality (provided by the operational environment per OE.CRYPTO).

Information collected from the managed elements is analyzed (FNM_ANL.1). The results of the analysis are available to 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 conditions detected on the managed elements (FNM_RCT.1). Alerts may cause notifications to be sent to configured destinations, scripts to be executed on the managed elements, or configuration files to be uploaded to the managed elements.

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

Access privileges for status and analysis information maintained by the Orion Server is determined by the user account privileges configured for each authorized Orion Server user account. Access privileges for status and configuration information maintained by the NCM Server is determined by the user account privileges configured for each authorized NCM Server user account. When an Orion Server Web Service user accesses NCM Server information, the NCM Integration Module acts as a proxy and transparently supplies the configured NCM user account credentials to the NCM Web Service on behalf of the Orion Server Web Service user.

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, FNM_STG.2). The TOE does not provide any direct database access to Orion Server Web Service, EOC Web Service, or NCM Web Service 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 administrators.

In the unlikely event that the storage capacity of the database is exhausted, the existing information in the database is maintained and new Monitor data is discarded.

7.1.4 Configuration Management

Relevant SFRs: FMT_MTD.1(2), FNM_ANL.1, FNM_RCT.1, FTP_ITC.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). 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). Configuration file uploads are protected (FTP_ITC.1), using cryptographic functionality (provided by the operational environment per OE.CRYPTO).

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). Configuration file uploads are protected (FTP_ITC.1), using cryptographic functionality (provided by the operational environment per OE.CRYPTO).

The TOE provides SFTP and SCP server functionality for configuration file downloads (FTP_ITC.1), using cryptographic functionality (provided by the operational environment per OE.CRYPTO).

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

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 and assumption is addressed by a security objective.

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

Table 17 - Threats and Assumptions to Security Objectives Mapping

	O.CHANNEL	O.CONFIG	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TOE_ACCESS	OE.COMM	OE.CRYPTO	OE.DATABASE	OE.DBMONITOR	OE.ENVIRON	OE.INSTALL	OE.INTROP	OE.NETWORK	OE.NOEVILADMIN	OE.SSL	OE.WINDOWSACCESS
A.ACCESS													X				
A.ASCOPE												X					
A.DATABASE									X								
A.ENVIRON											X						
A.INSTALL												X					
A.NETWORK														X			
A.NOEVILADMIN															X		
P.ACCESS			X			X											X
P.ANALYZ		X		X													
P.DBMONITOR										X							
P.DISCLOSURE	X						X	X								X	
P.INTGTY			X														
P.MANAGE						X											X
P.PASSWORDS					X												
T.MASQUERADE						X	X										X
T.TSF_COMPROMISE			X														

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

Table 18 - Threats, Assumptions and Policies to Security Objectives Rationale

x.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.DATABASE	The **OE.DATABASE** objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators 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.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 Orion 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	**O.CHANNEL** requires the TOE to use a trusted channel when sending credentials to a managed element. **OE.COMM** addresses the policy by requiring the environment to supply functionality to protect the communication between 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 protocols.
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 Orion Server functionality via Windows applications to users authorized to invoke TOE functionality.
P.PASSWORDS	**O.PASSWORDS** addresses this policy by requiring the TOE to provide functionality for Administrators, but not non-Administrators, to configure passwords.
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 TSF data from disclosure when it is transferred between distributed components of the TOE. **OE.WINDOWSACCESS** requires Windows to identify and authenticate users before they access Orion Server functionality via Windows applications.

x.TYPE	Security Objectives Rationale
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. **OE.OS_ PROTECTION** contributes to countering this threat by ensuring that the OS can protect itself from users within its control. If the OS could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the executable code of the TOE.

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 19 - SFRs to Security Objectives Mapping

	O.CHANNEL	O.CONFIG	O.MANAGE	O.MONITOR	O.PASSWORDS	O.TOE_ACCESS
FIA_ATD.1			X			X
FIA_UAU.2						X
FIA_UAU.7						X
FIA_UID.2						X
FIA_USB.1						X
FMT_MTD.1		X	X		X	
FMT_SMF.1			X			
FMT_SMR.1			X		X	
FNM_MDC.1		X		X		
FNM_ANL.1		X		X		
FNM_RCT.1				X		
FNM_RDR.1		X	X	X		
FNM_STG.1		X		X		
FNM_STG.2		X		X		
FTA_SSL.3						X
FTP_ITC.1	X					

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

Table 20 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.CHANNEL	**FTP_ITC.1** requires the TOE to use protected channels for specific operations that could otherwise expose sensitive data.
O.CONFIG	**FMT_MTD.1(*)** 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 upload, download, and compare configuration files for managed elements. **FNM_RDR.1** requires that configuration file comparisons (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. **FNM_STG.2** defines the behavior of the TOE if space in the database is not available to save a configuration file.
O.MANAGE	**FIA_ATD.1(*)** define the security attributes that must be able to be managed for users of the TOE. **FMT_MTD.1(*)** define the data access privileges associated with each role. **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported. **FNM_RDR.1** 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 configured conditions concerning the managed elements. **FNM_RDR.1** 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. **FNM_STG.2** defines the behavior of the TOE if space in the database is not available to save a configuration file.
O.PASSWORDS	**FMT_MTD.1(*)** define the access privileges for Administrators and non-Administrators, explicitly stating that only Administrators may configure passwords for User Accounts defined in the TOE. **FMT_SMR.1** defines the specific security roles to be supported.

Security Objective	SFR and Rationale
O.TOE_ACCESS	**FIA_ATD.1** defines the attributes of users, including a userid 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 userid 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 Orion Server Web Service 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(*)** 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 from part 3 of the Common Criteria.