WhatsUp Gold™ Premium
Version 16.1.99

Security Target

Version 1.0
January 27, 2014

Prepared for:

Ipswitch, Inc.

83 Hartwell Avenue
Lexington MA, 02421

Prepared By:

Leidos (formerly SAIC)
Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive
Columbia, MD 21046

and

Saffire Systems

P.O. Box 40295
Indianapolis, IN 46240

Table of Contents

List of Tables

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is WhatsUp Gold Premium with Plug-Ins Version 16.1.99, from Ipswitch, Inc. WhatsUp Gold™ Premium with Plug-Ins Version 16.1.99 is a network management and monitoring software product that monitors, reports, alerts, and takes action on the status of network devices, network services, and the network as a whole.

The Security Target contains the following additional sections:

- TOE Description (Section 2)—gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE
- Security Problem Definition (Section 3)—defines the security problem the TOE is intended to solve, in terms of threats to be countered by the TOE and its operational environment, and assumptions about the TOE's intended operational environment and method of use
- Security Objectives (Section 4)—specifies security objectives to be met by the TOE and its operational environment in order to solve the security problem defined in Section 3
- IT Security Requirements (Section 5)—presents the security functional requirements (SFRs) and security assurance requirements (SARs) for the TOE that are intended to achieve the security objectives specified in Section 4
- TOE Summary Specification (Section 6)—describes the security functions represented in the TOE that satisfy the SFRs presented in Section 5
- Protection Profile Claims (Section 7)—presents any Protection Profile claims and supporting rationale
- Rationale (Section 8)—closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – WhatsUp Gold™ Premium Version 16.1.99 Security Target

ST Version – Version 1.0

ST Date – January 27, 2014

TOE Identification – WhatsUp Gold Premium with Plug-Ins Version 16.1.99

TOE Developer – Ipswitch, Inc.

Evaluation Sponsor – Ipswitch, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 3, July 2009
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009
  - Part 3 Conformant.

This ST and the TOE it describes are conformant to the following package:

- EAL 2, augmented with ALC_FLR.1.

1.3 Conventions and Glossary

This section specifies the formatting conventions used in the Security Target and provides a list of abbreviations used throughout the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
    - Extended Requirements are allowed to create requirements should the Common Criteria not offer suitable requirements to meet the ST needs. To ensure these requirements are explicitly identified, the ending "_(EXT)" is appended to the newly created short name and the component.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Glossary

The following terms and abbreviations are used in this ST.

administrative user	In the context of this ST and the TOE it describes, 'administrative user' refers generally to either an underlying Windows account with administrator privilege or an Authorized User with the appropriate privileges (see below), i.e., some person with responsibility and authorization to perform administrative functions on the TOE.
AES	Advanced Encryption Standard—a symmetric encryption algorithm.
APC	American Power Conversion—an uninterruptible power supply (UPS) manufacturer
Authorized User	In the context of this ST and the TOE it describes, 'Authorized User' refers to a user with a WhatsUp Gold user account that defines the user's role in the TOE and determines the functions the user can perform. All Authorized Users access the TOE remotely via its web interface.
Cipher Suite	A cipher suite is a set of cryptographic algorithms. Cryptographic protocols in the TOE use algorithms from a cipher suite to create keys and perform cryptographic operations.

controlled object The TOE controls access to the following objects within its scope of control, based on user and access rights:

- Device object (or ‘device’)—a virtual representation of a resource (server, workstation, router, switch, etc.) connected to the network the TOE is monitoring.
- Device group—allows an Authorized User to organize the devices discovered on the network to assist monitoring and management.
- Monitor libraries— maintain a set of monitors that provide the means for an Authorized User to monitor the performance and behavior of network resources and of the network itself. There are 3 types of monitor libraries: active monitor library, passive monitor library, performance monitor library.
- Action library—maintains a set of actions that can perform a task as a device or monitor state change occurs. An Authorized User can configure an action to perform a specified task.
- Recurring Action library—maintains a set of recurring actions that provide the ability to fire actions based on a regular schedule, independent of the status of devices.
- Action Policy library—maintains a set of action policies that allow an Authorized User to group or sequence multiple actions together for use on any device or monitor. If changes are made to actions in a policy, the changes are applied to all of the devices and monitors that use that particular policy.
- Task library—maintains a set of tasks that are configured by an Authorized User to run a task script on a device.
- Task script library—maintains a set of task scripts that login to devices through SSH or Telnet and run command-line interface (CLI) commands on devices.
- Policy—a named collection of ASCII character strings that must or must not (as specified) appear in an archived device configuration file.
- Dashboard report—a configurable report display, specific to an Authorized User.
- Dashboard view—makes it possible for multiple reports to be viewed simultaneously by an Authorized User.
- Application Profile—groups components, discrete applications, and thresholds that capture data points into a template from which application instances can be created.
- Application Instance—a running copy of an application profile that monitors the defined collection of components, distinct applications, and thresholds necessary to define the health and performance of a given type of application.
- Flow source—a network device that uses one of the supported network monitoring protocols to send flow data to the Flow Monitor.
- Flow monitor—gathers, analyzes, and reports on network traffic patterns and bandwidth utilization of the flow sources.

DES Data Encryption Standard—a symmetric encryption algorithm. The TOE includes OpenSSL, which provides an implementation of Triple DES.

DNS Domain Name System—a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

GUI Graphical User Interface

HMAC Hash-based Message Authentication Code—an algorithm for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. The TOE includes OpenSSL, which provides an implementation of HMAC-SHA1.

HTML HyperText Markup Language

MIB Management Information Base—a computing information repository used by Simple Network Management Protocol (SNMP) and other implementations.

OID Object Identifier—in an SNMP context, consists of the object identifier for an object in a Management Information Base (MIB).

SHA Secure Hash Algorithm—a family of cryptographic hash functions. The TOE includes OpenSSL, which provides an implementation of SHA-1.

SMTP Simple Mail Transfer Protocol—an Internet standard for email transmission across Internet Protocol (IP) networks.

SNMP Simple Network Management Protocol—an Internet-standard protocol for managing devices on IP networks.

SSH Secure Shell

TLS Transport Layer Security

UPS Uninterruptible Power Supply

WCF Windows Communication Foundation—a runtime and a set of APIs in the .NET Framework for building connected, service-oriented applications.

WMI Windows Management Instrumentation—provides an operating system interface through which instrumented components provide information and notification, allowing system management information to be shared between management applications.

2. TOE Description

The Target of Evaluation (TOE) is WhatsUp Gold Premium with Plug-Ins Version 16.1.99 from Ipswitch, Inc (hereinafter referred to generally as WhatsUp Gold). It provides capabilities to discover devices on a network, monitor discovered devices, and execute actions on device state changes, enabling the network administrator to identify and act on network failures. It provides security management capabilities to manage and monitor the network. The security management capabilities are accessed via a web-based graphical user interface (GUI). The TOE can audit all logins and logouts of the GUI and many of the activities performed via the GUI. The TOE enforces role-based access control on the objects it defines that provide a logical representation of devices on the network. Authorized Users are identified and authenticated before gaining access to other capabilities of the TOE[1]. The TOE implements a password-based authentication mechanism. In addition, user accounts can be individually configured to use an external LDAP or Active Directory server for authentication of the claimed user identity.

2.1 TOE Overview

WhatsUp Gold is a network management product that discovers and monitors devices on the network and can detect changes in the status of monitored devices. Changes that cross configured thresholds can generate alerts, notifying the network administrator of device issues. Additionally, WhatsUp Gold can discover and monitor applications running on devices on the network.

WhatsUp Gold is available in three editions: Standard; Premium; and Distributed. Each edition tailors WhatsUp Gold's features to meet different deployment needs, from small networks to those spanning multiple geographic locations. Only the Premium Edition is included within the scope of the TOE. It provides all of the network management capabilities of WhatsUp Gold Standard Edition, and adds management for Microsoft Exchange, Microsoft SQL Server and SMTP mail servers. It also provides capabilities to monitor performance data and to monitor applications using Microsoft's Windows Management Instrumentation (WMI).

The TOE includes the following plug-ins (which can work with any of the WhatsUp Gold editions) that extend the monitoring and reporting capabilities of the base product:

- WhatsVirtual—an integrated plug-in for WhatsUp Gold that provides additional capabilities to discover, map, monitor, alert, and report on virtual environments, from small virtual environments hosted by a single VMware host to entire data centers managed by one or more VMware vCenter servers. With WhatsVirtual, one discovery scan can discover both virtual and physical devices. In Device View, virtual devices are displayed alongside physical devices. For each virtual host discovered, a group is created for the virtual host and all of its associated virtual machines. WhatsVirtual makes use of the VMware vSphere API to augment the mapping, reporting, monitoring, alerting, and notification capabilities of WhatsUp Gold.

- WhatsUp Gold Flow Monitor—makes use of Cisco NetFlow, sFlow, and J-Flow data from switches, routers, and Adaptive Security Appliances (ASA) to gather, analyze, report, and alert on LAN/WAN traffic patterns and bandwidth utilization in real-time. It highlights not only overall utilization for the LAN/WAN, specific devices, or interfaces, but also indicates users, applications, and protocols that are consuming abnormal amounts of bandwidth, providing information to assess network quality of service and resolve traffic bottlenecks.

- WhatsConfigured—supports management of device configurations by automating configuration and change management tasks required to backup, compare, and upload configuration files for networking devices. WhatsConfigured maintains and controls configuration files and alerts when any configuration changes are detected. WhatsConfigured is a web-based plug-in that ships as part of WhatsUp Gold Premium.

- WhatsUp Gold APM (Application Performance Monitoring)—this plug-in monitors applications across multiple devices, servers, and systems, providing performance statistics and overall application health, while alerting on performance degradation and potential problems before they result in service outages. APM assists in pinpointing application performance bottlenecks and points of failure.

[1] Note that devices on the network being monitored by the TOE are not considered "users" of the TOE.

The TOE also includes WhatsUp Gold Failover Manager, an application that provides user-configurable criteria to determine if WhatsUp Gold is in a failed state. The administrative user can choose to have the primary system go down if all services are disabled, or if any specified service is disabled.

The following sub-sections provide a general overview and description of product concepts and capabilities. Note that the specific capabilities covered by the evaluation are identified in the logical boundary discussion in Section 2.2.2. Additionally, section 2.2.2.9 describes optional applications that are not covered by the TOE evaluated configuration and section 2.2.2.10 describes features and capabilities of the TOE that are restricted from use in the evaluated configuration.

2.1.1 Devices

The TOE uses 'devices' to provide a virtual representation of the resources (servers, workstations, routers, switches, etc.) connected to the network it is monitoring. The TOE provides the capabilities to discover network resources (devices), manage their virtual representation within the TOE, monitor their performance, and generate alerts.

2.1.2 Network Discovery Scan

A network discovery scan is the process the TOE uses to identify devices on the network that are to be monitored. This process scans each device to determine its manufacturer, model, and running software and services. The TOE uses this information to automatically assign commonly used monitors to each device.

After the TOE discovers a device on an IP address, it queries the device to determine its manufacturer and model, components, operating system, and specific services. To gain this information, the TOE uses a combination of SNMP, WMI, and the VMware API. The discovery process uses SNMP, WMI and VMware credentials to correctly identify devices and these need to be configured on the TOE before starting a discovery scan.

When the TOE discovers devices, it tries to determine the type of each device so that it can monitor them appropriately. To determine a device type, the TOE compares the discovered attributes of each device to a set of criteria called device roles. Device roles are essentially attributes of a device. Device roles do two things:

- Specify the criteria that a device must match to be identified as the device role.
- Specify the monitoring configuration that is applied to the device when it is added to the TOE.

The TOE provides a number of pre-configured device roles that are used to identify most common network devices. If the network includes devices that are not identified by the pre-configured set, the administrative user can create custom device roles during the initial configuration using the Discovery Console within the Administration Console that is outside of the TOE. Creating custom device roles is outside the evaluated configuration. The TOE does provide the ability to manage the assignment of devices roles to a device managed by the TOE.

2.1.3 Device Groups

After the TOE discovers and identifies the role of a device, the Authorized User can add the device to a device group[2]. Device groups allow the Authorized User to organize the devices discovered on the network to assist monitoring and management.

After discovered devices are added to a device group, the TOE begins monitoring them immediately.

The TOE defines device group access rights to control which Authorized Users can manage specific groups and devices. There are four types of device group access rights:

- Group Read—allows Authorized Users to view groups and devices in a selected group. Also allows Authorized Users to see the group's map and device list.
- Group Write—allows Authorized Users to edit group properties and add, edit, and delete devices and subgroups within the selected group.
- Device Read—allows Authorized Users to view device properties of all devices within a selected group

[2] Note the number of devices that can be added to the TOE may be restricted by the product license.

- Device Write—allows Authorized Users to edit the device properties of any device within a selected group and to delete a device from the group.

2.1.4 Monitors

The TOE provides the following types of device monitors:

- Active Monitors—monitor the state of device entities, such as processes, ports, and services (Web servers, email servers, etc.).
- Passive Monitors—listen for device events, such as syslog events, SNMP traps, and Windows Event log entries.
- Performance Monitors—gather data about several performance components of the devices running on the network.
- Flow Monitors (provided by the WhatsUp Gold Flow Monitor plug-in)—use Cisco NetFlow, sFlow, and J-Flow data from switches, routers, and Adaptive Security Appliances (ASA) to gather, analyze, report, and alert on LAN/WAN traffic patterns and bandwidth utilization.

2.1.5 Application Discovery and Monitoring

In addition to discovering and monitoring devices on the network, the TOE can discover and monitor applications. From the perspective of the TOE, an application is made up of one or more components running on one or more monitored devices. The TOE defines three types of application:

- Simple application—an application that is not dependent on another application to run (e.g., Microsoft Server 2008 R2).
- Complex application—an application configured to be dependent on one or more applications to run (e,g., WhatsUp Gold requires IIS and SQL Server).
- Discrete application—an application upon which a complex application has a dependency. In the example above, IIS and SQL Server are discrete applications on which the complex application WhatsUp Gold is dependent.

The TOE monitors application status based on “components”—a component is a single data point that is collected by the TOE (e.g., CPU Utilization). In order to monitor an application, it is first necessary to create an application profile. An application profile defines a collection of individual components that reflect the health and status of a specific type of application. An application instance is a running copy of an application profile that monitors the defined collection of components and distinct applications. The TOE allows the Authorized User to create custom application profiles.

Application discovery can be performed manually any time after the network discovery scan is completed. The network device does not need to be configured before the application discovery can be performed. The application discovery feature scans for processes and services on the network device, as defined in the application profiles.

Application performance monitoring uses the active and performance monitors listed in Section 2.1.4 to provide its monitoring functionality.

2.1.6 Actions and Alerts

Actions are designed to perform a task as a device, application, or monitor state change occurs.

An Authorized User configures an action to perform a specified task. Actions can try to correct the problem, notify someone of the state change, or launch an external application. The Authorized User can assign the action to a device, an application, or to an active or passive monitor.

The Authorized User can configure actions on a single device, application, or monitor, or define an Action Policy to use across multiple devices, applications, or monitors. An Action Policy allows the Authorized User to group or sequence multiple actions together for use on any device, application, or monitor. If changes are made to actions in a policy, the changes are applied to all of the devices, applications, and monitors that use that particular policy.

In addition, the TOE supports the concept of Recurring Actions. These provide the ability to fire actions based on a regular schedule, independent of the status of devices. Among other things, this can be used to send regular heartbeat messages to an email address letting users know the system is up and running.

The TOE's Alert Center capability handles alerting on performance monitors, passive monitors, flow monitors, and the TOE's system health using the following mechanisms:

- Thresholds—these are the benchmark mechanisms Alert Center uses to check against the database. If the TOE finds that an aspect has exceeded or fallen below the parameters set in a threshold, it is considered out of threshold. These out of threshold aspects are logged as items. The Authorized User can find data for Alert Center items on the Alert Center Home page and in Alert Center reports.
- Notification Policies—when an aspect goes out of threshold and is logged as an item, associated notification policies begin sending notifications to alert administrative users of the problem. These policies can include multiple steps that begin at administrator-specified intervals to notify multiple people of persisting problems. After a problem is fixed, administrative users can be notified of the fix and subsequent steps of a running notification policy can be stopped.

Note that the TOE cannot guarantee delivery of notifications to external entities (e.g., via text message or email), or guarantee that an external application launched as part of an action will be successful in remediating a problem.

APM allows the administrator to configure action policies that can be applied to application instances and components being monitored. An action policy defines the actions to take when an application instance or component transitions from one state to another. State transition rules evaluate whether to permit the associated action to fire based on the amount of time the source was in a previous state. The action rules determine which action to fire and when to fire the action.

The TOE is designed to perform a number of actions in response to detected conditions. Of these, only the following have been evaluated:

- **Email Action**. Send an Email to a specific address.
- **SMS Action**. Send a text message to a specific target.
- **SSH Action**. Connect to remote devices via SSH to execute commands or scripts.

The following actions have not been evaluated:

- **Active Script Action**. Write code to perform a customized action.
- **Beeper Action**. Activate a beeper with this type of action.
- **Log to Text File**. Write a message to a text file.
- **Pager Action**. Send a message to a pager.
- **PowerShell Action**. Develop custom actions through direct access to scriptable component libraries, including the .NET Framework.
- **Program Action**. Execute an external application.
- **Service Restart Action**. Start or stop a Windows service.
- **SMS Direct**. Send a text message to a wireless phone or other wireless device.
- **SNMP Set**. Use SNMP to set the value of an attribute of a managed object.
- **Sound Action**. Play a specific sound.
- **Syslog Action**. Write a message to a log in the Syslog system.
- **Text to Speech Action**. Plays a voice message on your computer.
- **VMware Action**. Use the VMware API to perform an action on a virtual machine.
- **Web Alarm Action**. Activate a Web Alarm in the WhatsUp Gold Web Interface
- **Windows Event Log Action**. Write an event in the Windows Event Log.
- **Winpopup Action**. Send a Winpopup to a user or specific computer.

2.1.7 Tasks, Task Scripts, and Policies

The WhatsConfigured plug-in is built around an automated task execution engine that allows Authorized Users to dynamically gather configuration data about network devices through configuration tasks. These configuration tasks can be scheduled to run on a regular basis or can be manually run as needed to perform such tasks as uploading, downloading, and backing up configuration files, and managing device credentials. The TOE comes with several pre-defined configuration tasks with the option to create custom tasks. The Alert Center has the capability to alert on the success or failure of a task, or when changes are detected on a device.

The task is the controlled object that is configured by the Authorized User to run a task script on a device. Task scripts login to devices through SSH or Telnet and run command-line interface (CLI) commands on devices. These tasks can perform a number of operations, such as restoring or backing up a running or startup configuration, or changing an application password.

A policy is the controlled object that is configured by the Authorized User to search through archived configuration files for strings that are either expected or not expected within the file(s). Policies are added to Alert Center Task Thresholds. When a scheduled task fails a policy, any associated notification policies alert you that the policy has failed due to unexpected content that has been flagged in an archived configuration file.

Note that the evaluation covers only the access controls applied to tasks, task scripts, and policies as controlled objects. The efficacy of task scripts to perform tasks on devices and the efficacy of WhatsConfigured policies to detect patterns in archived configuration files have not been subject to evaluation.

2.1.8 Dashboards and Reports

A Dashboard is an administrator-specific, configurable reports display. A Dashboard contains multiple views that let the Authorized User organize various reports by the type of information they display.

The TOE provides the following Dashboard types:

- Home—can display both Home- and Device-level dashboard reports. The Authorized User can place any dashboard report on a Home dashboard, mixing and matching summary, group, and device-specific data.
- Device status—limited to display only Device-level dashboard reports. Only dashboard reports specific to a single device can be placed on a device dashboard. When the device-in-context is changed, the reports displayed show data corresponding to the newly selected device.
- Top 10—displays Top 10 full reports for network devices.

Each of the dashboard types supports multiple administrator-defined views and up to 15 small reports known as dashboard reports can be displayed within each view. These dashboard reports show content ranging from Current Interface and CPU utilization to Syslog messages. The TOE provides capabilities to manage dashboards and dashboard views.

The TOE supports two general types of report:

- Dashboard Reports—the TOE offers over 100 configurable dashboard reports for display in dashboard views. Dashboard reports can be Device dashboard or Home dashboard reports, depending on the dashboard type in which they can be displayed.
- Full Reports—used to troubleshoot and monitor performance and historical data that has been collected during the operation of the TOE.

2.1.9 Failover Support

The WhatsUp Gold Failover Manager provides the capability to automatically switch from a primary installation of WhatsUp Gold to a standby WhatsUp system when the primary system is not functioning normally.

The Failover Manager utilizes user-configurable criteria to determine a failed state. The TOE can be configured to have the primary system go down if all services are disabled, or if any specified service is disabled. For example, if the ‘all services’ option is configured, the services used by WhatsUp Gold must go down on the primary system for the secondary system to take over. Conversely, if only the Polling Engine and Web Server are configured, and both are disabled on the primary system for any reason, the secondary system takes over WhatsUp Gold network management duties until the primary system has been restored.

There are two scenarios supported by the WhatsUp Gold Failover Manager. Each scenario uses both a primary and secondary installation of WhatsUp Gold, with the database resident either on the secondary system (Scenario 1 – see Figure 1) or separately as its own system (Scenario 2 – see Figure 2). For both scenarios, the database must be located on a private physical network that is not globally routable and is protected from attacks and unauthorized physical access. Use of the Failover Manager in the TOE is optional.

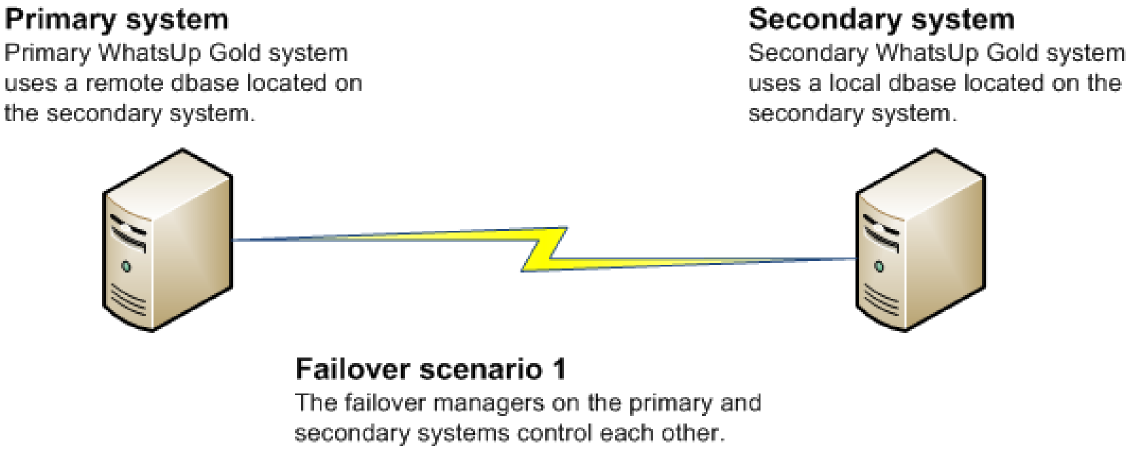
Primary system
Primary WhatsUp Gold system uses a remote dbase located on the secondary system.
Secondary system
Secondary WhatsUp Gold system uses a local dbase located on the secondary system.
Failover scenario 1
The failover managers on the primary and secondary systems control each other.

Figure 1: Failover Configuration with Database Collocated on Secondary System

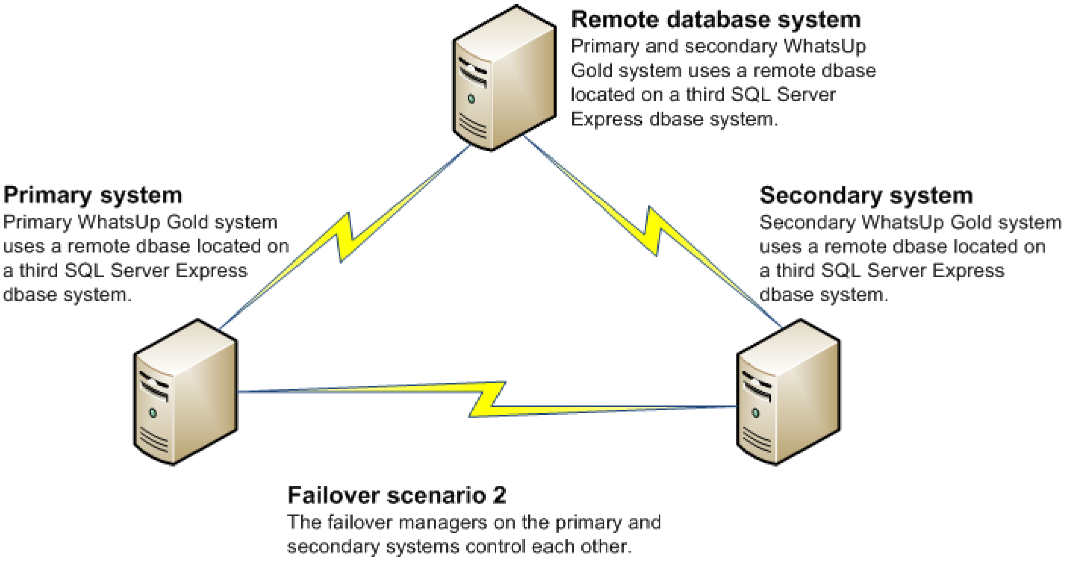
Remote database system
Primary and secondary WhatsUp Gold system uses a remote dbase located on a third SQL Server Express dbase system.
Primary system
Primary WhatsUp Gold system uses a remote dbase located on a third SQL Server Express dbase system.
Secondary system
Secondary WhatsUp Gold system uses a remote dbase located on a third SQL Server Express dbase system.
Failover scenario 2
The failover managers on the primary and secondary systems control each other.

Figure 2: Failover Configuration with Remote Database

2.2 TOE Architecture

2.2.1 Physical Boundaries

This section identifies the components comprising the TOE and the requirements the TOE has for hardware and software in its operational environment.

2.2.1.1 TOE Components

WhatsUp Gold consists of a number of services that operate within the context of a Windows operating system (see below for supported products). The services comprising WhatsUp Gold (including its plug-ins) are:

- Polling Engine (nmService.exe)
- Console (nmconsole.exe)
- Flow Collector (bwcollector.net.exe)
- Alert Center (alertcenterservice.exe)
- Whats Configured (networkconfigservice.exe)
- Discovery (discoveryservice.exe)
- Failover Manager (nmfailover.exe)
- API (nmapi.exe)
- Whats Connected Data Service (networkviewerdataservice.exe)
- Whats Virtual Service (whatsvirtualservice.exe)
- Service Bus (nmservicebus.exe)
- Polling Controller (nmpollingController.exe)
- Data Collector (nmdatacollector.exe)
- Active Monitor Manager (nmmanagers.exe)
- Poller (nmpoller.exe)
- Task Controller (nmtaskcontroller.exe)
- APM State Manager (apmstatemanager.exe)
- Wireless Poller (nmwireless.exe)
- WhatsUpConfiguration API (nmconfigurationmanager.exe)
- WhatsUp Message Server (nmmessageserver.exe)
- Action Manager (nmactionmanager.exe)
- Drone Manager (dronemanager.exe)
- APM Discovery (apmdiscoveryservice.exe)
- WhatsUp Gold Services Controller (NMServiceManager.exe)
- Trivial File Transfer Protocol Server (TFTPservice.exe).

In the evaluated configuration, WhatsUp Gold can be deployed with or without failover. If the Failover Manager is installed and configured, the TOE must be deployed in one of the two Failover scenarios described in Section 2.1.9 above. In addition, the TOE supports deployment of Remote Pollers, optional components that provide the means to extend WhatsUp Gold's polling capability, thus increasing the number of devices WhatsUp Gold can monitor. Remote pollers support active monitors and passive monitors and communicate with the WhatsUp Gold server over TLSv1.0 connections provided by .NET WCF (Windows Communication Foundation) in the operational environment.

2.2.1.2 Required Software and Hardware

The vendor supports WhatsUp Gold on the following Microsoft Windows platforms:

- Microsoft Windows Server 2008 R2 (64 bit)

- Microsoft Windows Server 2008 (32 bit and 64 bit)
- Microsoft Windows Server 2003 R2 (32 bit and 64 bit)
- Microsoft Windows Server 2003 (32 bit and 64 bit).

The vendor supports WhatsUp Gold operating on the following Windows operating systems, but recommends that it be installed on a server class operating system:

- Microsoft Windows 7 Professional and Ultimate editions (32 bit and 64 bit).

In addition, WhatsUp Gold will operate on any of the above supported operating systems running on the following virtual platforms:

- VMware ESX versions 3.5 and 4.x
- VMware ESXi 3.5 and 4.x
- Microsoft Hyper-V Server 2008 R2.

WhatsUp Gold remote pollers are supported on the same platforms as the WhatsUp Gold server.

WhatsUp Gold requires an external database to maintain data about monitored devices and applications, store system configurations, and save user specified customizations. The database may be co-located with the WhatsUp Gold installation, or may be hosted on a remote machine located on a private physical network that is not globally routable and is protected from attacks and unauthorized physical access. When the Failover Manager is installed and configured, this means that both WhatsUp Gold installations must be connected both to the private, protected network on which the database server is located and to the network(s) being monitored. Data services for WhatsUp Gold can be provided by the following supported database servers:

- Microsoft SQL Server 2008 R2 Express Edition 32-bit or 64-bit (shipped with WhatsUp Gold)
- Microsoft SQL Server 2005 Standard or Enterprise 32-bit or 64-bit
- Microsoft SQL Server 2008 or 2008 R2 Standard or Enterprise 32-bit or 64-bit
- Microsoft SQL Server Cluster 2005, 2008, or 2008 R2 Enterprise or Datacenter 32-bit or 64-bit (only for Windows Server deployments of WhatsUp Gold, and only in a remote configuration, i.e., installation of WhatsUp Gold on the same server as the database cluster is not supported).

Note that if the database shipped with the TOE (i.e., SQL Server 2005 Express Edition) is used, the size of the database is limited to 4 gigabytes. If the SQL Server 2008 Express R2 database is used, the size of the database is limited to 10 gigabytes.

Web services are required for the web-enabled functionality and reporting provided by WhatsUp Gold. These services can be provided by the following supported web servers:

- Microsoft Internet Information Services (IIS) version 6 (Windows Server 2003 deployments). This additionally requires the ASP (Active Server Pages) .NET web server extension.
- Microsoft IIS version 7.x (Windows 7 and Windows Server 2008 deployments). The TOE installation program automatically installs/enables IIS 7 on platforms where it is supported. Note that although the TOE requires Microsoft .NET Framework (see below), IIS 7.x requires the '.NET Framework Windows Communication Foundation (WCF) HTTP Activation' and 'Windows Communication Foundation (WCF) non-HTTP Activation' features/components **not** be enabled. When running with IIS 7.x, WhatsUp Gold additionally requires the following IIS Role Services: Web Server; ASP .NET; Static Content; HTTP Redirection; and Default Document.

WhatsUp Gold requires the Microsoft .NET Framework and other Microsoft packages to support scripting and software accessibility, as follows:

- Microsoft .NET Framework 4.0, included in the installation program
- Microsoft .NET Framework 2.0 or 3.0 or 3.5, required by the installation program (i.e., must already be installed prior to running TOE installation program)

- Microsoft Windows Scripting Host v5.7 or later
- Microsoft SAPI 5.1 (required for Text-to-Speech actions).

WhatsUp Gold supports the following browser clients for accessing the WhatsUp Gold Web interface: Microsoft Internet Explorer 7.0 and higher; Firefox 11 or higher; and Chrome 18 or higher.

The vendor identifies minimum recommended hardware requirements to support an installation of WhatsUp Gold in various configurations, as summarized in Table 1.

	100 Devices / 500 Monitors minimum recommended	**2,500 Devices / 12,500 Monitors minimum recommended**	**20,000 Devices / 100,000 Monitors minimum recommended**
Processor(s)	WhatsUp Gold: Dual-core (Physical computer recommended)	WhatsUp Gold: Quad-core (Physical computer recommended)	WhatsUp Gold Server: Eight-core Remote SQL Server: Eight-core (Physical computer recommended)
Processor speed	2.4 GHz or more	2.4 GHz or more	2.4 GHz or more
RAM	4 GB	8 GB	WhatsUp Gold Server: 8 GB Dedicated SQL Server: 32 GB (64 GB recommended)
Database type	SQL Server 2008 Express Edition	Dedicated Microsoft SQL Server 2005 / Microsoft SQL Server 2008 or 2008 R2 Standard 64-bit	Dedicated Microsoft SQL Server 2005 / Microsoft SQL Server 2008 or 2008 R2 Standard 64-bit
Hard drive	15 GB or more	**OS/Application** – 15 GB or more in RAID 1 **Database files** – 4 x 100 GB in RAID 10	**OS/Application** – 15 GB or more in RAID 1 **Database files** – 8 x 250 GB in RAID 10 **Log files** – 2 x 100 GB in RAID 0
Network interface card	100 Mbps (1 Gbps preferred)	100 Mbps (1 Gbps preferred)	1 Gbps
Video display resolution	1280 x 1024 or higher	1280 x 1024 or higher	1280 x 1024 or higher

Table 1: Minimum Recommended Hardware Capabilities for WhatsUp Gold

Regardless of configuration, the following capabilities have specific hardware requirements[3]:

- Installation from CD-ROM requires a CD-ROM or DVD-ROM drive.
- SMS actions require a modem and phone line (note that modem pooling is not supported).

The WhatsVirtual plug-in supports virtual hosts and virtual machines running on the following virtual environments:

- VMware vCenter Server 4.0, 4.1, and 5.0

[3] Note the following have additional hardware requirements: Text-to-Speech actions require a SAPI-capable sound card. Pager and Beeper actions require a modem and phone line. SMS Direct Actions required a GSM modem. These four actions that have additional hardware requirements are not included in the evaluated configuration.

- VMware ESX versions 3.5, 4.0, and 4.1
- VMware ESXi versions 3.5, 4.0, 4.1 and 5.0.

The WhatsUp Gold Flow Monitor plug-in has the same base requirements as WhatsUp Gold, but is more demanding on the database. In addition, in order to provide the capabilities described in this ST, WhatsUp Gold Flow Monitor requires at least one of the following in the operational environment:

- routing device that supports: NetFlow versions 1, 5, 7 and 9; sFlow versions 2 and 5; J-Flow; or IP Flow Information Export (IPFIX)
- a Flow Publisher monitoring a flow source (WhatsUp Flow Publisher, from Ipswitch, Inc., is a lightweight, passive, software agent that can be deployed to collect data from routers, switches, servers and other points of interest in the network and create flow data from the packet information—it is outside the TOE boundary).

The WhatsUp Gold Failover Manager application has the same base requirements as WhatsUp Gold, but requires additional hardware and software depending on the configured failover scenario. Deployment scenario 1 requires primary and secondary WhatsUp Gold machines, both of which meet all of the software and hardware requirements specified to support WhatsUp Gold. Deployment scenario 2 additionally requires a separate machine that meets the disk space requirements specified to support WhatsUp Gold. This machine runs a supported SQL Server database for remote use by both the primary and secondary WhatsUp Gold machines. Additionally, TCP Ports 9501 and 9643 are used by Failover Manager for communication between the primary and secondary machines, and for the nmapi.exe process.

WhatsUp Gold requires the following in its operational environment:

- Network devices must respond to ICMP echo request packets ("ping" packets) or TCP open port requests in order to be discovered by the TOE.
- Network devices must be configured to respond to SNMP or WMI requests in order for the TOE to be able to collect device information from them.
- Virtual network devices must be configured to respond to VMware vSphere API requests in order for the TOE to be able to collect device information from them.
- Authorized Users must use HTTPS when accessing the Web interface.

WhatsUp Gold can optionally be configured to use an LDAPv3 or Active Directory server (Windows Server 2008 R2 release) in its operational environment to support authentication of Authorized Users.

2.2.2 Logical Boundaries

This section describes the logical scope of the TOE, i.e., the logical security features offered by the TOE, in terms of the following security functions: Security Audit; Cryptographic Support; User Data Protection; Identification and Authentication; Security Management; Fault Tolerance; and Network Monitoring. In addition, this section identifies all capabilities to be provided by the operational environment, and those TOE capabilities excluded from the scope of evaluation.

2.2.2.1 Security Audit

The TOE generates audit records when Authorized Users logon to and logoff from the TOE via its web interface, and many of the activities performed by Authorized Users via the web interface. The audit records include the identity of the Authorized User performing the auditable action, the action performed by the Authorized User, and the date and time the audit record was generated. The TOE relies on its operational environment to provide a reliable time stamp for inclusion in the audit record. The TOE provides a means for Authorized Users with appropriate user rights to view the contents of the audit log.

Generated audit records are stored in the TOE's database maintained in the operational environment.

2.2.2.2 Cryptographic Support

The TOE includes the FIPS 140-2 validated version of the OpenSSL FIPS Object Module by Open Source Software Institute (OpenSSL version 0.9.8r, FIPS 140-2 certificate 1051) to provide cryptographic functions to support: SSHv2 sessions between the TOE and network devices; SNMPv3 communications between the TOE and network devices; TLSv1.0 communications between the TOE and an external authentication server; and secure storage of authentication credentials in the operational environment.

The TOE also relies on cryptographic capabilities provided by the operational environment. The TOE relies on the underlying operating system and web server for provision of HTTPS, which is required for Authorized Users to access the web interface of the TOE. The TOE also relies on .NET WCF in the operational environment to protect communications between WhatsUp Gold primary and secondary servers and between WhatsUp Gold server and remote pollers, using TLS.

2.2.2.3 User Data Protection

The TOE controls access by Authorized Users to the following controlled objects: device objects (the virtual representation of devices in the TOE); device groups; flow sources; flow monitors; monitor libraries; task library, task script library; action library; recurring action library; action policy library; dashboard views; dashboard reports; application profiles; and application instances. The TOE makes its access control decisions based on configured device group access rights, flow source access rights, and assigned user rights. Device group access rights are used to define access controls on devices and device groups. The access control policy does not apply to virtual devices accessed via the Virtual Map. Flow sources access controls are used to define access controls to flow sources. Assigned user rights are used to define access controls to all controlled objects, except flow sources.

2.2.2.4 Identification and Authentication

The TOE requires Authorized Users (who access the TOE via its web GUI) to be identified and authenticated before accessing any TOE functionality. In addition, the TOE supports external authentication using an LDAP or Active Directory server. Once logged on, Authorized Users are granted user rights that control their access to managed objects and determine what management actions they can perform. Users logged on to the TOE via the web interface have the capability to terminate their own interactive session.

2.2.2.5 Security Management

The TOE provides capabilities to manage the TOE’s features and security functions. The capabilities available to Authorized Users (defined as users who logon to the TOE via its web GUI, and who are identified and authenticated in the process) are restricted based on assigned user rights and configured device group access rights.

2.2.2.6 Fault Tolerance

The TOE provides the capability, through the WhatsUp Gold Failover Manager application, to determine if the TOE has entered a failed state and to subsequently recover the TOE to a fully operational state. The TOE can be configured to provide failover in the event all its services are disabled, or if any specified services are disabled. Use of failover in the evaluated configuration is optional.

2.2.2.7 Network Monitoring

The TOE provides the capabilities to discover network devices and applications, monitor the status of network devices and applications, generate alerts about the status of monitored network devices and applications, and perform actions in response to changes in the status of monitored network devices and applications.

In order for the Network Monitoring function to operate effectively, network devices must respond to ICMP echo request packets (“ping” packets) or open TCP port requests (in order to be discovered by the TOE), network devices must be configured to respond to SNMP or WMI requests (in order for the TOE to be able to collect device information), and virtual network devices must be configured to respond to VMware vSphere API requests (in order for the TOE to be able to collect device information from them).

The TOE relies on its operational environment for secure storage of scanning information, and the performance of device actions and alerts.

2.2.2.8 Capabilities to be Provided by the Operational Environment

The TOE relies on the operational environment for the following components and capabilities:

- The underlying operating system on which the TOE operates is relied on to provide domain separation for the various components of the TOE, to ensure they cannot be interfered with by other processes running on the same operating system.
- The underlying operating system is relied on to provide a secure file system to protect the TOE executables and data stored on the computer's disks, including data stored in the supporting database server.
- The supporting database server in the operational environment is relied on to provide secure storage of TSF data, including generated audit records.
- If the supporting database server is installed on a remote machine, the database must reside on a private physical network that is not globally routable and is protected from attacks and unauthorized physical access.
- The underlying operating system is relied on to provide a reliable time stamp for use by the TOE.
- The TOE stores some information (file paths, program settings) in the Windows registry and the underlying operating system is relied on to protect this information.
- The TOE relies on the underlying operating system and web server for provision of HTTPS, which is required for Authorized Users to access the Web interface of the TOE.
- The TOE relies on the underlying FIPS compliant operating system to provide cipher suite negotiation for SSHv2 and TLSv1.0 crypto operations performed by the TOE.
- The TOE relies on .NET WCF in the operational environment to provide secure communication (using TLSv1.0) between the WhatsUp Gold server and any deployed remote pollers, and between the WhatsUp Gold server primary and secondary instances.
- Network devices must respond to ICMP echo request packets ("ping" packets) or TCP open port requests in order to be discovered by the TOE.
- Network devices must be configured to respond to SNMP or WMI requests in order for the TOE to be able to collect device information from them.
- The TOE can optionally be configured to use an LDAP or Active Directory server in its operational environment to support authentication of Authorized Users.
- The TOE relies on the presence of a trustworthy Domain Name System (DNS) server in its operational environment to support hostname resolution.
- Virtual network devices must be configured to respond to VMware vSphere API requests in order for the TOE to be able to collect device information from them.

2.2.2.9 Product Capabilities not Covered by the Evaluation

The following features and capabilities of the TOE are not included within the scope of the evaluation:

- WhatsUp Gold WhatsConnected
- WhatsUp Log Management
- WhatsUp Gold VoIP Monitor
- AlertFox End-User Monitor
- WhatsUp Gold Flow Publisher
- IP Address Manager
- IP v6

The following features and capabilities of the TOE described in the guidance documentation are not included within the scope of the evaluation:

- Use of ELM (Event Log Management) tool to access ELM database functions
- Use of AlertFox for web server monitoring and reporting
- The efficacy of task scripts in performing operations on devices
- The efficacy of Active Script and SSH performance monitors
- The efficacy of actions in correcting problems detected on network devices
- The efficacy of send/expect language in the monitors
- Text-to-speech actions
- All notification actions except SMS and email

2.2.2.10 Product Capabilities Restricted from Use in the Evaluated Configuration

The following features and capabilities of the TOE described in the guidance documentation are restricted from use in the evaluated configuration:

- Use of the WhatsUp Gold console is excluded for regular operation of the TOE, since it is not subject to all of the access controls provided by WhatsUp Gold. In the evaluated configuration, the console is to be used only for the following tasks:
    - Initial installation and configuration of the TOE prior to the commencement of live operation, including:
        - configuring FIPS 140-2 mode
        - configuring device roles
        - configuring failover
    - Performing database maintenance, including backup and restore.
- Use of the Mobile interface to access the TOE.
- Use of the web GUI ‘Guest’ account, which is required to be deleted during installation in the evaluated configuration.
- Use of the dashboard application[4], which per guidance authorized administrators are instructed to not use.

2.3 TOE Documentation

Ipswitch offers installation and configuration guidance for WhatsUp Gold Premium, as well as guidance for subsequent use and administration of the applicable security features. The TOE documentation comprises the following:

- WhatsUp Gold Release Notes v16.1, March 12th, 2013
- WhatsUp Gold Getting Started Guide v16.1, March 8th, 2013
- Installing and Configuring WhatsUp Gold v16.1, March 11th, 2013
- Using Additional Pollers with WhatsUp Gold v16.1, June 24th, 2013
- WhatsUp Gold Online Help v16.1, April 2nd, 2013
- WhatsUp Gold v16.1 Database Migrations and Management Guide, June 18th, 2013
- Application Performance Monitoring for WhatsUp Gold v16.1 User Guide, February 28th, 2013

[4] The dashboard application is a separate software executable that is not to be confused with the dashboard that is visible within the WhatsUp Gold web GUI.

- WhatsUp Gold v16.1 Wireless User Guide, February 19th, 2013
- Flow Monitor for WhatsUp Gold v16.1 User Guide, February 19th, 2013
- WhatsVirtual for WhatsUp Gold v16.1 User Guide, February 15th, 2013
- Failover Manager for WhatsUp Gold v16.1 Quick Start Guide, March 11th, 2013
- WhatsUp Gold Failover Manager for WhatsUp Gold v16.1 Deployment and User Guide, March 12th, 2013
- WhatsUp Gold Premium Common Criteria Supplemental User Guidance, v2.1 January 14th, 2013.

3. Security Problem Definition

The security problem definition describes the security problem to be addressed by the TOE in the following terms:

- Threats that the TOE and the environment of the TOE counter
- Assumptions made about the operational environment and the intended method of use for the TOE.

Furthermore, the TOE is intended to be used in low threat environments where the relative assurance that its security functions are enforced is commensurate with EAL 2 augmented with ALC_FLR.1 as defined in the CC.

3.1 Assumptions

A.ADMIN The administrative users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

A.CREDEN Users granted authorization to logon to the TOE shall choose passwords that satisfy complexity requirements as specified in the guidance documentation.

A.DEV_COMMS The TOE and each device it monitors will be configured to use the most secure method of communication permitted by the particular device.

A.HTTPS The TOE will be configured so as to require the use of HTTPS to access its web-based management GUI.

A.INSTALL The TOE will be installed within the context of operating systems that provide the logical protection necessary to ensure the TOE cannot be tampered with or bypassed.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.PHYSICAL The computers on which the TOE is installed are located in physically secure areas such that access is restricted to authorized administrative users of the TOE.

A.RESPONSE Network devices to be monitored by the TOE are configured to respond to ping or open TCP port requests.

A.TOE_ONLY The computing system(s) on which the components of the TOE are installed are dedicated to its function and are not used for any other purpose.

3.2 Threats

In the threat statements listed below, these terms have the following meanings:

- Authorized User—as defined in the Glossary in Section 1.3.2 of this ST
- data—covers both user data (such as information the TOE gathers about servers, workstations, routers, etc.) and TSF data (used to enforce security policies)
- logical access—logical access is gained by establishing an interactive session with the TOE. It does not cover sending unsolicited or unacknowledged data to the TOE.

T.ACCESS Unauthorized entities may be able to gain logical access to the TOE and its data.

T.AUTHORITY Authorized Users may be able to perform actions for which they do not have authorization.

T.CONFIDENTIALITY An attacker may be able to observe TSF data that is stored in the IT environment or communicated to devices on the network.

T.DEVICE_STATUS The status of network devices may change, to the detriment of network operations, without the knowledge of network administrators.

T.FAILURE The capabilities of the TOE may become unavailable in the event one or more of its services fails.

T.UNACCOUNTABILITY Authorized Users may not be held accountable for their actions within the TOE, resulting in unauthorized and undetected activities that compromise the TOE or the data it protects.

4. Security Objectives

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats and address applicable assumptions.

4.1 Security Objectives for the TOE

O.ACCESS The TOE shall restrict access of Authorized Users to controlled objects, based on user privileges and object access rights.

O.AUDIT The TOE shall be able to log the activities of authorized users and shall provide capabilities to review logged activities.

O.FAILOVER The TOE shall provide the capability to failover to a backup system in the event of a failure of one or more of its services.

O.I&A The TOE shall be able to identify and authenticate authorized users that access the TOE remotely.

O.MANAGE The TOE shall provide capabilities to manage its security functions and shall restrict those capabilities to authorized users.

O.MONITOR The TOE shall provide capabilities to discover network devices, monitor the status of network devices, generate alerts about a monitored network device's status, and perform actions in response to changes in a monitored network device's status.

O.PROTECT The TOE shall provide mechanisms to protect the confidentiality of authentication credentials stored in the IT environment, communications between itself and network devices, and communications with the LDAP or AD server.

O.ROLES The TOE shall be able to associate Authorized Users of the TOE with the privileges that determine the access control and security management capabilities available to them.

4.2 Security Objectives for the Operational Environment

OE.ADMIN Those responsible for the TOE shall ensure the administrative users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

OE.CERTIFICATES The operational environment shall provide a means by which public key certificates can be created and managed.

OE.CREDEN Those responsible for the TOE shall ensure users granted authorization to logon to the TOE choose passwords that satisfy complexity requirements as specified in the guidance documentation.

OE.DB Those responsible for the TOE shall ensure the database is configured to protect the TSF data stored in it so that only the TOE can access the data.

OE.DEV_COMMS Those responsible for the TOE shall ensure the TOE and each device it monitors are configured to use the most secure method of communication permitted by the particular device.

OE.HTTPS Those responsible for the TOE shall ensure the TOE is configured so as to require the use of HTTPS to access its web-based management GUI.

OE.INSTALL Those responsible for the TOE shall ensure the TOE is installed within the context of operating systems that provide the logical protection necessary to ensure the TOE cannot be tampered with or bypassed.

OE.MANAGE Those responsible for the TOE shall ensure there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.

OE.PHYSICAL Those responsible for the TOE shall ensure the computers on which the TOE is installed are located in physically secure areas such that access is restricted to authorized administrative users of the TOE.

OE.RESPONSE Those responsible for the TOE shall ensure the network devices to be monitored by the TOE are configured to respond to ping or open TCP port requests.

OE.TIME The operational environment shall provide a reliable time stamp that can be used by the TOE.

OE.TOE_ONLY Those responsible for the TOE shall ensure the computing system(s) on which the components of the TOE are installed are dedicated to its function and are not used for any other purpose.

5. IT Security Requirements

This section specifies the security functional requirements satisfied by the TOE and the security assurance requirements against which the TOE is evaluated. The security functional requirements comprise requirements drawn from the CC Part 2 and extended security requirements that specify functionality not modeled by the CC. The security assurance requirements are precisely the requirements comprising the EAL2 assurance package, augmented with ALC_FLR.1.

5.1 Extended Component Definition

5.1.1 Network Monitoring (FNM)

This ST defines a new functional class for use within this ST: Network Monitoring (FNM). The ST author determined none of the existing CC Part 2 functional classes, families or components specifies requirements for a capability to discover network devices and applications, monitor the status of network devices and applications, generate alerts about the status of monitored network devices and applications, or perform actions in response to changes in such status.

5.1.1.1 Network Monitoring Device Discovery (FNM_DSC_(EXT))

This family defines requirements for being able to discover devices and applications on a network.

Management: FNM_DSC_(EXT).1

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

a) maintenance of the parameters that control network device scanning.

Management: FNM_DSC_(EXT).2

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

a) maintenance of the parameters that control device querying.

Management: FNM_DSC_(EXT).3

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

a) maintenance of the parameters that control scanning monitored network devices for applications.

Audit: FNM_DSC_(EXT).1, FNM_DSC_(EXT).2, FNM_DSC_(EXT).3

There are no auditable events foreseen.

FNM_DSC_(EXT).1: Network device discovery

Hierarchical to: No other components.

Dependencies: None

FNM_DSC_(EXT).1.1 The TSF shall be able to scan a network for devices using the following techniques: [**assignment:** ***non-empty list of scanning techniques***].

FNM_DSC_(EXT).2: Network device query

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_DSC_(EXT).2.1 The TSF shall be able to query discovered devices for [**assignment:** ***non-empty list of device information to be collected***] using the following techniques: [**assignment:** ***non-empty list of querying techniques***].

FNM_DSC_(EXT).3: Network application discovery

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_DSC_(EXT).3.1 The TSF shall be able to scan the monitored network devices for applications using the following criteria: [**assignment:** ***non-empty list of scanning criteria***].

5.1.1.2 Network Monitoring Capabilities (FNM_MNT_(EXT))

This family defines requirements for monitoring devices discovered on the network. Different types of monitoring, with different capabilities, are catered for in this family.

Management: FNM_MNT_(EXT).1, FNM_MNT_(EXT).2, FNM_MNT_(EXT).3, FNM_MNT_(EXT).4, FNM_MNT_(EXT).5

There are no management activities foreseen.

Audit: FNM_MNT_(EXT).1, FNM_MNT_(EXT).2, FNM_MNT_(EXT).3, FNM_MNT_(EXT).4, FNM_MNT_(EXT).5

There are no auditable events foreseen.

FNM_MNT_(EXT).1: Supported monitor types

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_MNT_(EXT).1.1 The TSF shall provide [**selection:** ***active, passive, performance, flow, [assignment: other types of monitor]***] monitors to monitor the network and devices discovered on the network.

FNM_MNT_(EXT).2: Active monitor capabilities

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_MNT_(EXT).2.1 The TSF shall be able to query devices on the network for the status of the following types of service [**assignment:** ***non-empty list of services***].

FNM_MNT_(EXT).2.2 Based on the response returned by a queried device, the TSF shall report the service as “up” if the expected response is returned, and shall report the service as “down” if an unexpected response or no response is returned.

FNM_MNT_(EXT).3: Passive monitor capabilities

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_MNT_(EXT).3.1 The TSF shall be able to collect the following events generated by devices on the network: [**selection:** ***SNMP traps, Syslog messages, Windows Event Log events, [assignment: other types of event]***].

FNM_MNT_(EXT).3.2 The TSF shall generate a record of each collected event that includes at least the following information: the date and time the event was detected; the event source; and any information recorded in the event by its source.

FNM_MNT_(EXT).4: Performance monitor capabilities

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_MNT_(EXT).4.1 The TSF shall be able to collect the following performance-related data from devices on the network: [**assignment:** ***non-empty list of performance characteristics***].

FNM_MNT_(EXT).4.2 The TSF shall be able to generate reports of performance-related data for individual devices and device groups that include at least the following information: the date and time range the device was monitored; the device identity; the performance data collected from the identified device.

FNM_MNT_(EXT).5: Flow monitor capabilities

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery

FNM_MNT_(EXT).5.1 The TSF shall be able to collect network flow data produced by the following protocols [**selection:** ***NetFlow, sFlow, JFlow, IPFIX, [assignment: other network flow protocols]***], including: network interfaces through which data flows; protocols; source identifiers; destination identifiers.

FNM_MNT_(EXT).5.2 The TSF shall be able to generate reports of flow-related data for individual interfaces that include at least the following information: sender; receiver; protocol.

5.1.1.3 Network Monitoring Actions and Alerts (FNM_ACT_(EXT))

This family defines requirements for performing actions and generating alerts based on state changes of monitors and monitored devices.

Management: FNM_ACT_(EXT).1

There are no management activities foreseen.

Management: FNM_ACT_(EXT).2

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

a) maintenance (creation, modification, deletion) of alerts.

Management: FNM_ACT_(EXT).3

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

a) maintenance (creation, modification, deletion) of notification policies.

Audit: FNM_ACT_(EXT).1, FNM_ACT_(EXT).2, FNM_ACT_(EXT).3

There are no auditable events foreseen.

FNM_ACT_(EXT).1: Actions

Hierarchical to: No other components.

Dependencies: FNM_DSC_(EXT).1 Network device discovery,
FNM_MNT_(EXT).1 Supported monitor types

FNM_ACT_(EXT).1.1 The TSF shall be able to associate actions with [**selection:** ***devices, active monitors, passive monitors, applications***].

FNM_ACT_(EXT).1.2 The TSF shall be able to perform an action when the criteria to trigger the action are satisfied.

Application Note: *The intent of this element is that the TSF can do something that causes the monitored device to do something (e.g., the TSF can send a command to the device that the device will itself interpret and execute), rather than to do something directly on the monitored device.*

FNM_ACT_(EXT).2: Alerts

Hierarchical to: No other components.

Dependencies: FNM_MNT_(EXT).1 Supported monitor types

FNM_ACT_(EXT).2.1 The TSF shall be able to associate alerts with [**selection:** ***performance monitors, passive monitors, flow monitors***].

FNM_ACT_(EXT).2.2 The TSF shall be able to identify when a monitored aspect exceeds or falls below its alerting threshold.

FNM_ACT_(EXT).2.3 The TSF shall generate a log when a monitored aspect is outside of its threshold that includes: date and time; device identity; threshold; aspect identity; aspect value.

FNM_ACT_(EXT).3: Notifications

Hierarchical to: No other components.

Dependencies: FNM_ACT_(EXT).2 Alerts

FNM_ACT_(EXT).3.1 The TSF shall be able to associate notification policies with alerting thresholds.

FNM_ACT_(EXT).3.2 The TSF shall support the following notification mechanisms: [**selection:** ***email, SMS, [assignment: other notification mechanisms]***].

FNM_ACT_(EXT).3.3 When an alerting threshold is exceeded, the TSF shall apply any notification policy associated with the exceeded threshold.

5.2 TOE Security Functional Requirements

The following table identifies the security functional requirements that are satisfied by WhatsUp Gold Premium.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_SAR.3: Selectable audit review
	FAU_STG.3: Action in case of possible audit data loss
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1(1): Cryptographic operation
	FCS_COP.1(2): Cryptographic operation
	FCS_COP.1(3): Cryptographic operation
	FCS_COP.1(4): Cryptographic operation
	FCS_COP.1(5): Cryptographic operation
	FCS_COP.1(6): Cryptographic operation
	FCS_COP.1(7): Cryptographic operation
FDP: User Data Protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.2: User identification before any action

Requirement Class	Requirement Component
FMT: Security Management	FMT_MOF.1(1): Management of security functions behavior
	FMT_MOF.1(2): Management of security functions behavior
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1(1): Management of TSF data
	FMT_MTD.1(2): Management of TSF data
	FMT_MTD.1(3): Management of TSF data
	FMT_MTD.1(4): Management of TSF data
	FMT_MTD.1(5): Management of TSF data
	FMT_MTD.1(6): Management of TSF data
	FMT_MTD.1(7): Management of TSF data
	FMT_MTD.1(8): Management of TSF data
	FMT_MTD.1(9): Management of TSF data
	FMT_MTD.1(10): Management of TSF data
	FMT_MTD.1(11): Management of TSF data
	FMT_MTD.1(12): Management of TSF data
	FMT_MTD.1(13): Management of TSF data
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_FLS.1: Failure with preservation of secure state
FRU: Resource utilisation	FRU_FLT.2: Limited fault tolerance
FTA: TOE Access	FTA_SSL.4: User-initiated termination
FNM: Network Monitoring	FNM_DSC_(EXT).1: Network device discovery
	FNM_DSC_(EXT).2: Network device query
	FNM_DSC_(EXT).3: Network application discovery
	FNM_MNT_(EXT).1: Supported monitor types
	FNM_MNT_(EXT).2: Active monitor capabilities
	FNM_MNT_(EXT).3: Passive monitor capabilities
	FNM_MNT_(EXT).4: Performance monitor capabilities
	FNM_MNT_(EXT).5: Flow monitor capabilities
	FNM_ACT_(EXT).1: Actions
	FNM_ACT_(EXT).2: Alerts
	FNM_ACT_(EXT).3: Notifications

Table 2: TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit data generation (FAU_GEN.1)

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

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

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

c) [**Authorized User logons, Authorized User logoffs, specifically defined auditable events listed in Table 3**].

Requirement	Auditable Events
FMT_MSA.1	Modify Access Control List
FMT_MTD.1(1)	Query, modify, delete, create user accounts
	Query, modify, delete, create user groups
FMT_MTD.1(2)	Change a user's own password
FMT_MTD.1(3)	Modify credentials library
FMT_MTD.1(4)	Query, modify, delete, create alerts (a.k.a. Alert Center Threshold Library)
FMT_MTD.1(6)	Modify, create credentials for connecting to an LDAP authentication server
FDP_ACF.1	Create, edit, remove active monitor
	Create, edit, remove passive monitor
	Create, edit, remove performance monitor
	Create, edit, remove flow monitor
	Create, edit, remove action
	Create, edit, remove recurring action
	Create, edit, remove action policy
	Create, edit, remove dashboard view
	Create, edit, remove dashboard report
	Edit device
	Create, edit, remove device group

Table 3: Security Functional Requirements and Auditable Events

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the action performed by the Authorized User**].

5.2.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**Authorized Users with 'Access System Reports' User Right**] with the capability to read [**all audit information**] from the audit records.

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

5.2.1.4 Restricted audit review (FAU_SAR.2)

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

5.2.1.5 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [**sorting**] of audit data based on [**date and time, subject identity**].

5.2.1.6 Action in case of possible audit data loss (FAU_STG.3)

FAU_STG.3.1 The TSF shall **[notify an Authorized User]** if the audit trail exceeds **[90% of the storage capacity of the underlying server]**.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ANSI X9.31 Appendix A.2.4 PRNG**] and specified cryptographic key sizes [**128, 192, 256 bits for AES; 168 bits for 3DES**] that meet the following: [**ANSI X9.31**].

5.2.2.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key `destruction method [**overwrite with zeroes**] that meets the following: [**FIPS 140-2**].

5.2.2.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1(1) The TSF shall perform [**symmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CBC, 3DES in CBC**] and cryptographic key sizes [**128, 192, 256 bits for AES; 168 bits for 3DES**] that meet the following: [**FIPS PUB 197 (AES); FIPS PUB 46-3 (3DES)**].

FCS_COP.1.1(2) The TSF shall perform [**cryptographic signature services**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024 bits**] that meet the following: [**FIPS PUB 186-3**].

FCS_COP.1.1(3) The TSF shall perform [**cryptographic key agreement services**] in accordance with a specified cryptographic algorithm [**Diffie-Hellman**] and cryptographic key sizes [**1024 bits**] that meet the following: [**RFC 2631**].

FCS_COP.1.1(4) The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA1**] and ~~cryptographic key~~ **digest** sizes [**160 bits**] that meet the following: [**FIPS PUB 180-3**].

FCS_COP.1.1(5) The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm [**HMAC-SHA1**] and cryptographic key sizes [**512 bits**] that meet the following: [**FIPS PUB 198**].

FCS_COP.1.1(6) The TSF shall perform [**SSH v2.0**] in accordance with ~~a~~ **the** specified cryptographic algorithm**s** [**3DES/AES, HMAC-SHA1, RSA, Diffie-Hellman**] and cryptographic key sizes [**168 (3DES)/128/192/256 bits (AES), 1024 bits (RSA), 512 bits (HMAC-SHA1), and 1024 bits (Diffie-Hellman)**] that meet the following:[**3DES/AES (see FCS_COP.1(1)), RSA (see FCS_COP.1(2)), HMAC-SHA1 (see FCS_COP.1(5)), Diffie-Hellman (see FCS_COP.1(3)), and SSHv2.0 (Transport Layer – RFC 4253, User Authentication Layer – RFC 4252, Connection Layer – RFC 4255)**].

FCS_COP.1.1(7) The TSF shall perform [**TLS v1.0**] in accordance with ~~a~~ **the** specified cryptographic algorithm**s** [**3DES/AES, SHA1, RSA**] and cryptographic key sizes [**168 (3DES)/128/192/256 bits (AES), 1024 bits (RSA), not applicable for SHA1**] that meet the following:[**3DES/AES (see FCS_COP.1(1)), RSA (see FCS_COP.1(2)), SHA1 (see FCS_COP.1(4)), and TLS v1.0 (RFC 2246)**].

5.2.3 User Data Protection (FDP)

5.2.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**Access Control SFP**] on [

- **Subjects: Authorized Users;**
- **Objects: Device Group Objects (device group, devices)**[5]**, flow sources, active monitor library, passive monitor library, performance monitor library, flow monitor, task library, task script library, policy, action library, recurring action library, action policy library, dashboard view, dashboard report, application profile, application instance;**
- **Operations: see Table 4 and Table 5**].

5.2.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [

- **Authorized Users: User Rights, User Groups**
- **Device Group Objects, flow sources: Access Control List (a list of User/User Group and Access Rights pairs)**

Note that access to all objects, except devices, device groups, and flow sources, is governed only by User Rights assigned to the Authorized User].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
An Authorized User's effective access rights are a combination of all User Rights assigned to their user account and all User Rights assigned to any user groups of which their user account is a member.

If Device Group Access Rights are not enabled, permitted operations on all objects except flow sources are determined only by User Rights. In order to perform a requested operation on an object, an Authorized User must be assigned the applicable User Right (either directly or via user group membership), as specified in Table 4.

Object	Operation	User Right
device accessed via device list	**add to device group, edit properties, clone**	**Manage Devices**
device group accessed via device list	**create, edit properties, remove**	**Manage Device Groups**
device accessed via Wireless tab	**view**	**Access Wireless**
device group accessed via Wireless tab	**view**	**Access Wireless**
active monitor library	**view, create, edit, remove**	**Configure Active Monitors**
passive monitor library	**view, create, edit, remove**	**Configure Passive Monitors**
performance monitor library	**view, create, edit, remove**	**Configure Performance Monitors**
flow monitor	**configure**	**Configure Flow Monitor**

[5] This access policy applies to all devices accessed via the Devices list and to wireless devices accessed via the Wireless tab. Virtual devices access via the Virtual tab are not subject to this access control policy.

Object	Operation	User Right
task, task script library, policy	view, configure, delete	Configure WhatsConfigured Tasks
action library	view, create, edit, remove	Configure Actions
recurring action library	view, create, edit, remove	Manage Recurring Actions
action policy library	view, create, edit, remove	Configure Action Policies
dashboard view	add, delete, copy, edit properties	Manage Dashboard Views
dashboard report	configure, move, delete	Configure Dashboards
application profile	view, create, edit, copy, delete	Configure APM Application Profiles
application instance	create, edit, delete	Configure APM Application Instances

Table 4: Required User Rights

If Device Group Access Rights are enabled, access to Device Group Objects is restricted to the device groups to which the Authorized User has access. Access to a device group is determined by the Access Control List associated with the device group, which specifies the Device Group Access Rights each Authorized User or User Group has to the device group and the objects within the device group.

Operations on the device group and devices in the device group are further restricted based on the specific Device Group Access Rights assigned in the Access Control List, as specified in Table 5.

Operation accessed via the Device list unless otherwise noted	Access Rights
list group, map group	GR
create group, edit group properties	GR/GW
copy group	GR on source, GR/GW on destination
move group	GR/GW on source, GR/GW on destination
delete group	GR/GW/DR/DW on group and all subgroups and devices
create device	GR/GW/DR/DW; if device already exists in other groups, GR/GW/DR/DW in at least one of those groups
copy device	GR on source, GR/GW on destination; device level rights must be same in both groups, except that downgrade from DR/DW to DR is permitted
move device	GR/GW on source, GR/GW on destination; device level rights must be same in both groups, except that downgrade from DR/DW to DR is permitted
view device properties	DR

Operation accessed via the Device list unless otherwise noted	Access Rights
modify device properties, acknowledge device	DR/DW
KEY: GR – Group Read; GW – Group Write; DR – Device Read; DW – Device Write	

Table 5: Device Group Access Rights

When a device exists in more than one device group, the group access rights from all groups are added together to determine the rights granted to the Authorized User.

To access flow source data within the flow monitor, the user must have access rights to that flow source. The access rights for flow sources are either access allowed or access denied.

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**an Authorized User has full access to any dynamic groups contained in a device group for which the Authorized User is assigned Device Group Access Rights**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**If Device Group Access Rights are enabled and an Authorized User is assigned no Device Group Access Rights to a device group, the Authorized User has no access to the device group or any of its objects**].

5.2.4 Identification and Authentication (FIA)

5.2.4.1 User attribute definition (FIA_ATD.1.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **User Name**
- **Authentication Type (Internal or LDAP)**
- **Password (if Authentication Type is Internal)**
- **Home Device Group**
- **User Groups**
- **User Rights**].

5.2.4.2 User authentication before any action (FIA_UAU.2)

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

5.2.4.3 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [**a local authentication mechanism and shall support a remote authentication mechanism**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

- **If the user account associated with the user identity to be authenticated specifies an Authentication Type of LDAP, the TSF shall provide the submitted password to a configured external LDAP server and enforce the authentication decision returned by the LDAP server. If the TSF cannot establish communication with the LDAP server, the remote user shall be unable to login**
- **If the user account associated with the user identity to be authenticated specifies an Authentication Type of Internal, the TSF shall use the submitted password to authenticate the claimed user identity**].

5.2.4.4 User identification before any action (FIA_UID.2)

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

5.2.5 Security Management (FMT)

5.2.5.1 Management of Security Functions Behaviour (FMT_MOF.1(1))

FMT_MOF.1.1(1) The TSF shall restrict the ability to [***determine the behavior of, modify the behavior of***] the functions [**Access Control SFP**] to [**Authorized User with 'Manage Users' User Right**].

5.2.5.2 Management of Security Functions Behaviour (FMT_MOF.1(2))

FMT_MOF.1.1(2) The TSF shall restrict the ability to [***determine the behavior of, modify the behavior of, enable, disable***] the functions [**Network Discovery Scan**] to [**Authorized User with 'Access Discovery Console' User Right**].

5.2.5.3 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***query, modify***] the security attributes [**Access Control List**] to [**Authorized User with 'Manage Users' User Right**].

5.2.5.4 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Access Control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Authorized User with 'Manage Users' User Right**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.5 Management of TSF Data (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to **[*query, modify, delete, [create]*]** the **[user accounts, user groups]** to [**Authorized User with 'Manage Users' User Right]**.

5.2.5.6 Management of TSF Data (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to **[*modify*]** the **[user's own password]** to [**Authorized User with 'Change Your Password' User Right]**.

5.2.5.7 Management of TSF Data (FMT_MTD.1(3))

FMT_MTD.1.1(3) The TSF shall restrict the ability to **[*query, modify*]** the **[Credentials Library]** to [**Authorized User with 'Configure Credentials' User Right]**.

5.2.5.8 Management of TSF Data (FMT_MTD.1(4))

FMT_MTD.1.1(4) The TSF shall restrict the ability to **[*query, modify, delete, [create]*]** the **[alerts, notification policies]** to [**Authorized User with 'Configure Alert Center' User Right]**.

5.2.5.9 Management of TSF Data (FMT_MTD.1(5))

FMT_MTD.1.1(5) The TSF shall restrict the ability to **[*modify*]** the **[global email settings]** to [**Authorized User with 'Email Settings' User Right]**.

5.2.5.10 Management of TSF Data (FMT_MTD.1(6))

FMT_MTD.1.1(6) The TSF shall restrict the ability to **[*query, modify, delete, [create]*]** the **[credentials for connecting to an LDAP authentication server]** to [**Authorized User with 'Configure LDAP Credentials' User Right]**.

5.2.5.11 Management of TSF Data (FMT_MTD.1(7))

FMT_MTD.1.1(7) The TSF shall restrict the ability to **[*modify*]** the **[Alert Center Threshold items]** to [**Authorized User with 'Administer Alert Center Threshold Items' User Right]**.

5.2.5.12 Management of TSF Data (FMT_MTD.1(8))

FMT_MTD.1.1(8) The TSF shall restrict the ability to **[*[manage global settings for]*]** the **[wireless devices]** to [**Authorized User with 'Configure Wireless' User Right]**.

5.2.5.13 Management of TSF Data (FMT_MTD.1(9))

FMT_MTD.1.1(9) The TSF shall restrict the ability to **[*perform actions on*]** the **[virtual devices]** to [**Authorized User with 'Access Virtualization Actions Menu' User Right]**.

5.2.5.14 Management of TSF Data (FMT_MTD.1(10))

FMT_MTD.1.1(10) The TSF shall restrict the ability to **[*query*]** the **[virtual devices accessed via the Virtual Map]** to [**Authorized User with 'Access WhatsVirtual Map' User Right]**.

5.2.5.15 Management of TSF Data (FMT_MTD.1(11))

FMT_MTD.1.1(11) The TSF shall restrict the ability to **[*view*]** the **[virtual device report]** to [**Authorized User with 'Access WhatsVirtual' User Right]**.

5.2.5.16 Management of TSF Data (FMT_MTD.1(12))

FMT_MTD.1.1(12) The TSF shall restrict the ability to **[*copy*]** the **[dashboard view into another user's dashboard]** to [**Authorized User with 'Manage Dashboard View' User Right]**.

5.2.5.17 Management of TSF Data (FMT_MTD.1(13))

FMT_MTD.1.1(13) The TSF shall restrict the ability to **[*create, edit, copy, delete*]** the **[APM Application Profiles and APM Application Instances]** to [**Authorized User with 'Access APM' User Right]**.

5.2.5.18 Specification of Management Functions (FMT_SMF.1)

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

- **Management of user accounts**
- **Manage Credentials Library**
- **Manage global email settings**
- **Manage LDAP credentials**
- **Perform a discovery scan of the network**
- **Manage alerts and notification policies**
- **Enable/disable Device Group Access Rights**
- **Manage Access Control List**
- **Manage Alert Center Threshold items**
- **Manage wireless devices**
- **Manage virtual devices**
- **Manage APM application profiles and instances**
- **Manage Dashboards**].

5.2.5.19 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles: [**Authorized User with one or more of the following User Rights:**

- **Access System Reports**

- **Manage Users**
- **Change Your Password**
- **Email Settings**
- **Configure LDAP Credentials**
- **Configure Credentials**
- **Configure Alert Center**
- **Access Discovery Console**
- **Administer Alert Center Threshold Items**
- **Configure Wireless**
- **Access Virtualization Actions Menu**
- **Access WhatsVirtual Map**
- **Access WhatsVirtual**
- **Access APM**
- **Access Layer-2**
- **Manage Layer-2**].

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

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Failure with Preservation of Secure State (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**failure of TOE services as specified during configuration of the TOE, if the Failover Manager is installed and configured**].

5.2.7 Resource Utilization (FRU)

5.2.7.1 Limited Fault Tolerance (FRU_FLT.2)

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [**failure of TOE services as specified during configuration of the TOE, if the Failover Manager is installed and configured**].

Application Note*: The "TOE services" in FPT_FLS.1 and FRU_FLT.2 refer to the specific Windows services listed in Section 2.2.1.1 that comprise the TOE. The TOE can be configured to provide failover in the event all its services are disabled, or if any specified services are disabled.*

5.2.8 TOE Access (FTA)

5.2.8.1 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

5.2.9 Network Monitoring (FNM)

5.2.9.1 Network Device Discovery (FNM_DSC_(EXT).1)

FNM_DSC_(EXT).1.1 The TSF shall be able to scan a network for devices using the following techniques: [**ICMP, TCP open port**].

5.2.9.2 Network Device Query (FNM_DSC_(EXT).2)

FNM_DSC_(EXT).2.1 The TSF shall be able to query discovered devices for [**manufacturer, model, components, operating system, Services**] using the following techniques: [**SNMP, WMI, VMware API**].

5.2.9.3 Network Application Discovery (FNM_DSC_(EXT).3)

FNM_DSC_(EXT).3.1 The TSF shall be able to scan the monitored network devices for applications using the following criteria: [**application profiles**].

5.2.9.4 Supported Monitor Types (FNM_MNT_(EXT).1)

FNM_MNT_(EXT).1.1 The TSF shall provide [***active, passive, performance, flow, [no other types]***] monitors to monitor the network and devices discovered on the network.

5.2.9.5 Active Monitor Capabilities (FNM_MNT_(EXT).2)

FNM_MNT_(EXT).2.1 The TSF shall be able to query devices on the network for the status of the following types of service [**DNS, Windows Service, TCP/IP Service, Telnet, SMTP, FTP, HTTP, SQL Server**].

FNM_MNT_(EXT).2.2 Based on the response returned by a queried device, the TSF shall report the service as "up" if the expected response is returned, and shall report the service as "down" if an unexpected response or no response is returned.

5.2.9.6 Passive Monitor Capabilities (FNM_MNT_(EXT).3)

FNM_MNT_(EXT).3.1 The TSF shall be able to collect the following events generated by devices on the network: [***SNMP traps, Syslog messages, Windows Event Log events***].

FNM_MNT_(EXT).3.2 The TSF shall generate a record of each collected event that includes at least the following information: the date and time the event was detected; the event source; and any information recorded in the event by its source.

5.2.9.7 Performance Monitor Capabilities (FNM_MNT_(EXT).4)

FNM_MNT_(EXT).4.1 The TSF shall be able to collect the following performance-related data from devices on the network: [**CPU Utilization, Disk Utilization, Interface Utilization, Memory Utilization, Ping latency and availability, statistical output power usage, Printer, SNMP performance counters, WMI performance counters**].

FNM_MNT_(EXT).4.2 The TSF shall be able to generate reports of performance-related data for individual devices and device groups that include at least the following information: the date and time range the device was monitored; the device identity; the performance data collected from the identified device.

5.2.9.8 Flow Monitor Capabilities (FNM_MNT_(EXT).5)

FNM_MNT_(EXT).5.1 The TSF shall be able to collect network flow data produced by the following protocols [***NetFlow, sFlow, Jflow, IPFIX***], including: network interfaces through which data flows; protocols; source identifiers; destination identifiers.

FNM_MNT_(EXT).5.2 The TSF shall be able to generate reports of flow-related data for individual interfaces that include at least the following information: sender; receiver; protocol.

5.2.9.9 Actions (FNM_ACT_(EXT).1)

FNM_ACT_(EXT).1.1 The TSF shall be able to associate actions with [***devices, active monitors, passive monitors, applications***].

FNM_ACT_(EXT).1.2 The TSF shall be able to perform an action when the criteria to trigger the action are satisfied.

5.2.9.10 Alerts (FNM_ACT_(EXT).2)

FNM_ACT_(EXT).2.1 The TSF shall be able to associate alerts with [***performance monitors, passive monitors, flow monitors***].

FNM_ACT_(EXT).2.2 The TSF shall be able to identify when a monitored aspect exceeds or falls below its alerting threshold.

FNM_ACT_(EXT).2.3 The TSF shall generate a log when a monitored aspect is outside of its threshold that includes: date and time; device identity; threshold; aspect identity; aspect value.

5.2.9.11 Notifications (FNM_ACT_(EXT).3)

FNM_ACT_(EXT).3.1 The TSF shall be able to associate notification policies with alerting thresholds.

FNM_ACT_(EXT).3.2 The TSF shall support the following notification mechanisms: [***email, SMS***].

FNM_ACT_(EXT).3.3 When an alerting threshold is exceeded, the TSF shall apply any notification policy associated with the exceeded threshold.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.1: Basic flaw remediation
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 6: EAL2 augmented with ALC_FLR.1 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Security-enforcing Functional Specification (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic Modular Design (ADV_TDS.1)

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIS trace to the behavior described in the TOE design that they invoke.

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer’s delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle Support (ALC)

5.3.3.1 Use of a CM System (ALC_CMC.2)

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1C The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM Coverage (ALC_CMS.2)

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery Procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.4 Basic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Analysis of Coverage (ATE_COV.1)

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 Functional Testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent Testing – Sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability Analysis (AVA_VAN.2)

AVA_VAN.2.1D The developer shall provide the TOE for testing.

AVA_VAN.2.1C The TOE shall be suitable for testing.

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the TOE security functions.

6.1 TOE Security Functions

The TOE implements the following security functions that together satisfy the SFRs claimed in Section 5.2 of this ST:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Fault Tolerance
- Network Monitoring.

6.1.1 Security Audit

The TOE generates audit records when Authorized Users logon to and logoff from the TOE via its web interface, and for the activities identified in Table 3 performed by Authorized Users via the web interface. In addition, the TOE audits the startup and shutdown of each of its services, including the Ipswitch Services Control Manager (ISCM). The ISCM controls all component services and controls the audit function for the TOE. Therefore, auditing the startup and shutdown of the ISCM audits the startup and shutdown of the audit function. The audit records include: date and time of the auditable event (obtained from the operational environment); the event category (i.e., event type); the identity of the Authorized User associated with the event (i.e., the subject identity); and the specific details associated with the event, including an indication of the outcome (success or failure) of the event.

The generated audit events for web user actions are recorded in the Web User Activity Log, which is one of the System reports produced by the TOE. Audit records not generated due to a web user action, including startup and shutdown events, are stored in the Logger Log. Both logs are stored in the TOE's database maintained in the operational environment.

In the evaluated configuration, the TOE is configured to monitor the server on which its database is installed. This enables the TOE to monitor the database's server for disk exhaustion and to initiate assigned notification policies in the event the available disk space drops below 10% of capacity. The notification policy alerts an Administrative User to take appropriate actions to increase the space available for storing audit records (e.g., backup and then delete audit records in the TOE database). The necessary configuration steps are described in the *WhatsUp Gold Premium Common Criteria Supplemental User Guidance*.

Authorized Users with the **Access System Reports** user right are able to view the contents of the Web User Activity Log and the Logger Log. The Authorized User is able to sort the contents of the log based on the date and time field or the Authorized User identity (i.e., subject identity).

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TSF generates audit events for the events defined and records the specified information in the audit log.
- FAU_GEN.2: The TSF is able to associate each auditable event with the identity of the user that caused the event.
- FAU_SAR.1: The TSF provides Authorized Users with the **Access System Reports** user right with the capability to read all audit information from the audit records. The TSF provides the audit records in a manner suitable for the user to interpret the information.

- FAU_SAR.2: The TSF prohibits all users read access to the audit records, except those users that have been granted explicit read-access (i.e., Authorized Users with the **Access System Reports** user right).
- FAU_SAR.3: The TSF provides the ability to sort audit data based on the date-time stamp and the Authorized User identity.
- FAU_STG.3: When configured in accordance with its guidance documentation, the TSF is able to monitor the storage capacity of the server hosting the TOE's database and notify an Authorized User in the event the available disk space drops below 10% of capacity.

6.1.2 Cryptographic Support

The TOE includes OpenSSL version 0.9.8r to provide cryptographic functions to support:

- SSHv2 sessions between the TOE and network devices
- SNMPv3 communications between the TOE and network devices
- TLS v1.0 sessions between the TOE and an external authentication server
- Secure storage of credentials in the operational environment.

The TOE also includes the OpenLDAP 2.4.25 library to implement the TLS v1.0 protocol using the cryptographic functions in OpenSSL. In the evaluated configuration, the external authentication server (LDAP or AD server) is configured to use TLS to protect communications between itself and WhatsUp Gold.

The TOE supports a FIPS 140-2 mode of operation and will automatically place itself in FIPS 140-2 mode if it detects it is installed on a FIPS compliant operating system. Ipswitch uses the OpenSSL FIPS object module v1.2 exactly as delivered by the Open Source Software Institute and built it according to documented instructions found in the Security Policy. The contents of the distribution file were not manually modified during the build process. WhatsUp Gold invokes FIPS 140-2 approved as described in the Security Policy ensuring all security functions and cryptographic algorithms are performed in FIPS 140-2 approved mode.

The TOE automatically generates symmetric keys for encrypting and decrypting session data once an SSHv2 session has been established with the network device. These keys are automatically destroyed by the TOE, by overwriting with 0's, when the session is terminated. Cipher suite negotiation for symmetric keys generated by the TOE for use in SSHv2 and TLSv1.0 protocols is performed within the operational environment. The administrator may need to configure the FIPS compliant operating system by modifying the priority of FIPS algorithms and key sizes to be negotiated if a lower priority key and length (such as 168-bit 3DES) needs to be provided by the TOE.

The following tables identify the cryptography provided by the TOE and its use.

Cryptographic Method	Use within SSHv2
SP 800-56 Key Exchange	Used in SSHv2 session establishment.
RSA Digital Signatures	Used in SSHv2 session establishment.
ANSI X9.31 PRNG	Used in SSHv2 session establishment.
HMAC-SHA1	Used to provide SSHv2 traffic integrity verification.
3DES/AES	Used to encrypt SSHv2 session traffic

Table 7: SSHv2 Related Cryptography

Cryptographic Method	Use within SNMPv3
HMAC-SHA	Used for initial authentication
AES (128 bit)	Used to encrypt SNMPv3 session traffic.

Table 8: SNMPv3 Related Cryptography

Cryptographic Method	Use within TLS v1.0

RSA Digital Signatures	Used in TLSv1.0 session establishment.
ANSI X9.31 PRNG	Used in TLSv1.0 session establishment.
SHA-1	Used to provide TLSv1.0 traffic integrity verification.
3DES/AES	Used to encrypt TLSv1.0 session traffic

Table 9: TLSv1.0 Related Cryptography

Additionally, the TOE uses 256-bit AES to encrypt the authentication credentials that it stores in its database.

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE generates symmetric keys to support AES and Triple DES cryptographic operations.
- FCS_CKM.4: The TOE destroys cryptographic keys by overwriting them with zeroes
- FCS_COP.1(1): The TOE implements AES and Triple DES to provide symmetric encryption and decryption services
- FCS_COP.1(2): The TOE implements RSA (with 1024 bit keys) to provide digital signature generation and verification services in support of SSH
- FCS_COP.1(3): The TOE implements Diffie-Hellman to provide cryptographic key agreement services
- FCS_COP.1(4): The TOE implements SHA1 to provide cryptographic hashing services.
- FCS_COP.1(5): The TOE implements HMAC-SHA1 to provide keyed-hash message authentication services.
- FCS_COP.1(6): The TOE implements SSHv2 using the cryptographic capabilities specified in FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3) and FCS_COP.1(5).
- FCS_COP.1(7): The TOE implements TLS v1.0 using the cryptographic capabilities specified in FCS_COP.1(1), FCS_COP.1(2) and FCS_COP.1(4).

6.1.3 User Data Protection

The TOE controls access by Authorized Users to monitor libraries, action library, recurring action library, action policy library, task library, task script library, dashboard views, dashboard reports, application profiles, and application instances, based on assigned user rights. The TOE controls access by Authorized Users to device objects and device groups, based on assigned user rights and configured device group access rights. The access control policy defined in this section does not apply to virtual devices when accessed via the Virtual Map. The TOE controls access by Authorized Users to flow sources, based on the object's access control list.

6.1.3.1 Controlled Objects

Device objects (or 'devices') provide a virtual representation of the resources (servers, workstations, routers, switches, etc.) connected to the network the TOE is monitoring. The TOE provides the capabilities to discover network resources (devices), manage their virtual representation within the TOE, monitor their performance, and generate alerts.

Device groups allow the Authorized Users to organize the devices discovered on the network to assist monitoring and management.

Monitors provide the means for Authorized Users to monitor the performance and behavior of network resources and of the network itself. The TOE supports four types of monitor: active; passive; performance; and flow. The flow monitor gathers, analyzes, and reports on network traffic patterns and bandwidth utilization of network devices (called flow sources).

Actions are designed to perform a task as a device or monitor state change occurs. The Authorized User configures an action to perform a specified task. Actions can try to correct the problem, notify someone of the state change, or launch an external application. The Authorized User can assign the action to a device, or to an active or passive monitor.

Recurring Actions provide the ability to fire actions based on a regular schedule, independent of the status of devices.

Action Policies allow the Authorized Users to group or sequence multiple actions together for use on any device or monitor. If changes are made to actions in a policy, the changes are applied to all of the devices and monitors that use that particular policy.

Tasks are configured by the Authorized Users to run a task script on a device. Task scripts login to devices through SSH or Telnet and run command-line interface (CLI) commands on devices. Tasks scripts contain command(s) which may be sequenced to automate the execution of administrative tasks on CLI-supported devices. The administrator has the ability to create and schedule task scripts that are invoked by the TOE on a regular or as needed basis. Examples of tasks scripts are backing up or restoring a running or startup configuration. The TOE supports the following protocols for downloading configuration information to a target system: SNMP; SSH; telnet; and TFTP. TFTP is disabled by default and enabled only when associated with a task. When a task performs a configuration operation via TFTP, it is associated with the specific IP address of the target system, and disabled once the operation has been completed. Guidance will instruct Authorized Users to avoid any other general use of the Ipswitch TFTP server as TFTP is an insecure protocol.

WhatsConfigured policies augment the above-mentioned tasks by allowing the Authorized User to specify exact strings that must or must not exist in an archived device configuration file. Policies can specify plain ASCII text strings or regular expressions. Authorized Users attach a configured policy to an Alert Center threshold which is associated with a device that is accessible to the Authorized User. If a threshold is breached, the specified configuration file is evaluated against the configured policy.

A dashboard is a configurable reports display, specific to an Authorized User. A dashboard contains multiple views that let the Authorized User organize various dashboard reports by the type of information they display.

6.1.3.2 User Rights

User rights govern what actions Authorized Users can perform on the TOE. Some user rights control security management capabilities (see Section 6.1.5) while the rest control access to objects and are one of the mechanisms supporting the TOE’s access control policy. The user rights related to access control are described in the following table.

Access Right	Description
Manage Dashboard Views	Enables user to add, delete and copy dashboard views, as well as edit properties of a specific dashboard view
Configure Dashboards	Enables user to modify a dashboard view by configuring, moving, and deleting dashboard reports within the dashboard view
Configure Active Monitors	Enable user to create, edit, and remove active monitors on devices in the groups to which the user has access
Configure Passive Monitors	Enables user to create, edit and remove passive monitors on devices in the groups to which the user has access
Configure Performance Monitors	Enables user to create, edit and remove performance monitors on devices in the groups to which the user has access
Configure Flow Monitor	Enables user to create, edit and delete Flow Monitor sources, collection intervals, and data intervals for reports
Configure WhatsConfigured Tasks	Enables user to configure WhatsConfigured tasks and task scripts on devices in the groups to which the user has access and to configure policies on archived device configuration files

Access Right	Description
Configure Actions	Enables user to create, edit, and remove actions on devices in the groups to which the user has access
Manage Recurring Actions	Enables user to create, edit, and remove recurring actions on devices in the groups to which the user has access
Configure Action Policies	Enables user to create, edit and remove action policies on devices in the groups to which the user has access
Manage Devices	Enables user to use the Devices list to add new devices and edit existing devices in the groups to which the user has access. This includes the ability to manage the device roles assigned to a device.
Manage Device Groups	Enables user to use the Devices list to create, edit, or remove device groups on the network
Configure APM Application Profiles	Enables users to create, modify, and delete application profiles. Note: The Access APM user right is needed to access the APM workspace in order to configure the APM application profiles.
Configure APM Application Instances	Enables users to create, modify, and delete application instances. Note: The Access APM user right is needed to access the APM workspace in order to configure the APM application instances.
Access Wireless	Enables users to monitor devices identified as wireless infrastructure devices via the Wireless tab

Table 10: User Data Protection Access Rights

An Authorized User has the set of user rights assigned directly to their user account and additionally inherits all user rights assigned to the user groups of which their user account is a member.

6.1.3.3 Device Group Access Rights

Device group access rights enable WhatsUp Gold users to see or make changes to specific device groups and devices that are accessed via the Devices list and via the Wireless tab. These rights can be enabled or disabled by an Authorized User with the **Manage Users** user right and are disabled by default.

Device group access rights are useful when users need to view and edit only those groups that matter to them, as would be the case with a large network with multiple network administrators. Device group access rights allow an Authorized User to grant each user rights to only the devices on the network for which that user is responsible, except for virtual devices accessed via the Virtual Map.

There are four types of device group access rights:

- **Group Read**—allows users to view groups and devices in the selected group accessed from the Devices list. This right allows users to see the group's map and device list. Group-level reports are not affected by group access rights but are affected by user rights. Within the Wireless tab, this right is necessary to see the existence of the devices and device groups.
- **Group Write**—allows users to edit group properties and add, edit, and delete devices and subgroups within the selected group.
- **Device Read**—allows users to view the device properties of all devices within the selected group. Device-level reports are not affected by group access rights but are affected by user rights.
- **Device Write**—allows users to edit the device properties of any device within the selected group and to delete the device from the group.

6.1.3.4 Flow Source Access Rights

Flow source access rights define which users can access the flow source. The access rights for flow sources are either access allowed or access denied. The flow source access rights are used to access flow source data within the Flow Monitor.

6.1.3.5 Access Control Policy

If device group access rights are not enabled, Authorized Users potentially have access to all device groups and devices. In this case, permitted operations to all objects except flow sources are determined only by user rights. Access rights for flow sources are always in effect and are not controlled by whether or not device group access rights are enabled or disabled.

When device group access rights are enabled, WhatsUp Gold determines effective rights by first negotiating user rights, then group access rights. This means that, while device group access rights govern access to device groups, a user must first have user access rights to a device or group before group access rights are considered. For example, if a user does not have the **Manage Devices** user right, then Device Write group access rights are not honored.

Device group access rights are assigned per device group by specifying the specific rights to the device group for each Authorized User or user group defined in the TOE. That is, each device group has associated with it a list of all Authorized Users and user groups and, for each, the specific device group access rights (if any) granted to that user or user group. An Authorized User that is not assigned any device group access rights to a device group has no access to the device group or any of its objects (unless an object in the device group is a member of another device group—see below). The access control policy does not apply to virtual devices accessed via the Virtual Map.

When device group access rights are initially enabled, the Administrator account (refer to Section 6.1.5.2) has full rights to all objects subject to device group access rights and all other user accounts have no rights, so only the Administrator account can access objects initially due to the default ACL.

Group access rights are passed from parent group to subgroup. When a new group is created, all of the group access rights defined for the parent group are inherited by the new group. The TOE also provides the capability to propagate changes made to rights on a parent group to all subgroups recursively.

Devices can belong to more than one device group, and each group can specify a different set of group access rights. When a device exists in multiple groups, the group access rights from all of the groups are added together to determine the rights granted to an authorized user when accessing the device. This is illustrated in the following table.

	Device Read	**Device Write**
Rights granted user in Device Group A	X	-
Rights granted user in Device Group B	-	X
Rights granted user in Device Group C	-	-
Effective rights when accessing device from any group	X	X

Table 11: Effective Device Group Access Rights

In this example, the user has Device Read access due to the device’s membership of Device Group A and Device Write access due to the device’s membership of Device group B, even though the user has no rights to Device Group C.

The following is a list of operations and the group access rights that must be assigned for the user to perform that task:

- List and Map in the Group Views menu require Group Read access.
- Create Group and Group Properties in the Group Operations menu require Group Read and Group Write access.
- Copy Group requires Group Read in the source group, and Group Read and Group Write in the destination group. (Note that this operation also copies the permissions to the group and its sub-groups. Since a copy of

an existing group is being made in a new location, the copy does not inherit permissions from its new parent).

- Move Group requires Group Read and Group Write in both the source and the destination groups. (Permissions of the group and sub-groups remain the same.)
- Delete Group requires Group Read, Group Write, Device Read, and Device Write recursively. (Device Read Write may not be required if the group is empty).
- Create Device requires Group Read, Group Write, Device Read, and Device Write. If the device already exists in other group(s), you must also have Group Read, Group Write, Device Read, and Device Write in one or more of those groups.
- Copy Device requires Group Read in the source group and Group Read and Group Write in the destination group. The level of device permissions must be the same in both groups. Downgrade from Device Read and Device Write to Device Read is also permitted.
- Move Device requires Group Read and Group Write in both the source and the destination groups. The level of device permissions must be the same in both groups. Downgrade from Device Read and Device Write to Device Read is also permitted.
- Viewing Device Properties requires Device Read.
- Modifying Device Properties, Bulk Field Change, and Acknowledgement require Device Read and Device Write.

Authorized users can be assigned a Home device group and are given Group Read rights to their Home device group by default.

Having access to configure monitors used by the device is distinct from having access to the data collected from the device as displayed by the monitors. The following items can be assigned to a device (which corresponds to editing the properties of a device): active monitors, passive monitors, performance monitors, actions, action policies, tasks. The 'Manage Devices' user right is the only user right needed to perform the following operations on items assigned to a device:

- add an item from the library to the device
- delete an item from the device
- modify the device-specific parameters of the item on the device, such as changing the polling interval parameter.

Assigning an item to a device means that the item can be used on/by the device; it does not imply access to configure/edit the item itself. Access to the item's library is required to configure/edit the item. Once assigned to a device, access to the results of assigning that item to the device is controlled by the access rights on the device. For example, if an active monitor is assigned to device A, a user with access to device A can view the output of the monitor even though the user does not have 'Configure Active Monitor' user right and cannot view the contents of, create, edit or remove the active monitor definition in the active monitor library.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1, FDP_ACF.1: The TOE controls access to device objects (the virtual representation of devices in the TOE) and device groups that are accessed via the Devices list and Wireless tab, based on configured device group access rights and assigned user rights. The Wireless Map cannot be accessed unless a user has been granted the "Access Wireless" user right. The access control policy does not apply to virtual devices accessed via the Virtual Map. The TOE controls access to the monitor libraries, task library, task script library, action library, recurring action library, action policy library, dashboard views, dashboard reports, application profiles, and application instances based on assigned user rights. The TOE controls access to flow sources based on configured flow source access rights.
- FMT_MOF.1(1): The TOE restricts to Authorized Users with the **Manage Users** user right the ability to manage the behavior of the Access Control SFP.

- FMT_MSA.1: The TOE restricts to Authorized Users with the **Manage Users** user right the ability to manage the ACLs used to enforce the Access Control SFP.
- FMT_MSA.3: Device group access rights are disabled by default, so Authorized Users can perform operations for which they have the appropriate user rights on any objects within the scope of the SFP. In this way, the default values for security attributes are considered permissive. The TOE restricts to Authorized Users with the **Manage Users** user right the ability to specify initial values for the ACLs.

  All wireless capabilities provided by the TOE are controlled by an access control policy or restricted for use by security management user rights.

6.1.4 Identification and Authentication

Authorized Users access the TOE via its web interface. An Authorized User connects to the web interface using any supported browser (as listed in Section 2.2.1). The web interface is hosted on an IIS server in the TOE's operational environment and can be accessed via HTTP or HTTPS (HTTPS is required in the evaluated configuration). Users logged in to the TOE via its web interface are able to terminate their own interactive sessions by logging out.

The TOE requires Authorized Users to be identified and authenticated before accessing any TOE functionality. The TOE implements its own password-based authentication mechanism. In addition, the TOE supports external authentication using an LDAP or Active Directory server. Once logged on, Authorized Users are granted user rights that control their access to controlled objects and determine what management actions they can perform.

The TOE defines and maintains user accounts for Authorized Users. Each user account defines the following attributes:

- User name—identifies the Authorized User
- Authentication type—can be Internal (the TOE maintains the user's password and authenticates the user's identity) or LDAP (an external LDAP or Active Directory server is used to authenticate the user's identity)
- Password—the password the TOE uses to authenticate the user's identity (if the Authentication type is Internal)
- User rights—defines the actions (security management and access control) the user is authorized to perform on the TOE
- User groups—specify the user groups of which this account is a member. User groups can be assigned user rights (just as individual user accounts) and a user account inherits all the user rights from each group of which it is a member
- Home device group—the device group the user sees when logging on at the web interface.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE maintains the following list of security attributes belonging to individual Authorized Users: user name, authentication type, password, user rights, user groups, and home device group.
- FIA_UAU.2: The TOE requires each Authorized User (i.e., a user accessing the TOE via its web interface) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.5: The TOE provides local and remote authentication mechanisms to support authentication of Authorized Users. The TOE authenticates any user's claimed identity according to the following rules: if the Authorized User account specifies LDAP authentication, the TOE provides the submitted password to a configured external LDAP server and enforces the authentication decision returned by the LDAP server. If the TOE cannot establish communication with the LDAP server, the Authorized User is unable to login. If the Authorized User account specifies Internal authentication, the TOE uses the submitted password to authenticate the user.
- FIA_UID.2: The TOE requires each Authorized User (i.e., a user accessing the TOE via its web interface) to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

- FTA_SSL.4: The TOE allows user-initiated termination of each user’s own interactive session.

6.1.5 Security Management

6.1.5.1 User Rights

The TOE provides capabilities to manage the TOE’s features and security functions. The capabilities available to Authorized Users (defined as users who logon to the TOE via its web GUI, and who are identified and authenticated in the process) are restricted based on assigned user rights and configured device group access rights.

User rights govern what actions Authorized Users can perform on the TOE. Some user rights control access to objects and are one of the mechanisms supporting the TOE’s access control policy (see Section 6.1.3), while the rest control security management capabilities. The user rights related to security management are described in the following table.

Name	Description
Access System Reports	Enables user to view System reports (including the Web User Activity Log)
Manage Users	Enables user to create and edit users for the web interface and to specify Group Access Rights Also having the Manage Dashboard View access control user right enables users to add, delete and copy dashboard views, as well as edit properties of a specific dashboard view. This right grants access to all features and functionality in the WhatsUp Gold web interface. Enabling this right enables all user rights.
Change Your Password	Enables user to change user’s own password
Email Settings	Enables user to configure email settings
Configure LDAP Credentials	Enables user to configure LDAP credentials for connecting to an LDAP server for user authentication in the web interface
Configure Credentials	Enables user to configure all credentials as listed in Section 6.1.5.3.
Configure Alert Center	Enables user to create, edit, and delete Alert Center thresholds and notification policies
Access Discovery Console	Enables user to access the Discovery Console. Granting users access to this dialog also enables users to discover network devices and add them to the TOE database
Administer Alert Center Threshold Items	Enables users to resolve or acknowledge Alert Center Threshold alerts
Configure Wireless	Enables users to manage wireless infrastructure devices within WhatsUp Gold Wireless. Note the “Configure Wireless” right has a dependency on the “Access Wireless” right. That is a user must have access to Wireless via the “Access Wireless’ right in order to be able to configure wireless.
Access Virtualization Actions Menu	Enables users to perform VM actions (stop, pause, restart, etc) on any virtual host within WhatsUp Gold
Access WhatsVirtual Map	Enables users to list the virtual devices and view statistics for each virtual device accessed via the Virtual Map
Access WhatsVirtual	Enables users to view the virtual device reports.
Access APM	Enables users to view and access the APM workspace in order to configure APM application profiles and APM application instances.
Access Layer-2	Enables users to view all Layer 2 data, including reports and tools.

Name	Description
Manage Layer-2	Enables users to use all Layer 2 Group/Map manipulation features, including Map properties and right-click map operations.

Table 12: Security Management User Rights

The TOE also defines user rights that are not security-related in the context of this ST (i.e., they do not contribute to the enforcement of any SFRs). They are described in the following table.

Name	Description
Translations	Enables user to view the translation system as well as import and export languages
Access Group and Device Reports	Enables user to view group and device reports for the groups the user can access
Access SSG Reports	Enables users to view Split Second Graph reports in the workspace and full reports
Create Scheduled Reports	Enables user to configure Scheduled Reports
Manage Scheduled Reports	Enables user to manage and view other user’s Scheduled Reports
Access Remote Reports	Enables users to view reports on TOE remote sites
Configure Remote Sites	Enables users to create, edit and delete remote sites
Access Alert Center Reports	Enables user to view Alert Center reports. Note that while the “Access Alert Center Reports” user right is not security relevant on its own, it is required in conjunction with the “Administer Alert Center Threshold Items” user right to provide the Authorized user with the ability to view the page before they can actually resolve the alert.
Access Flow Monitor Reports	Enables user to view Flow Monitor reports
Manage SNMP MIBs	Enables user to download and delete SNMP MIBs
E-mail Reports	Enables users to email an exported report to a specific email address.
Manage Business Hours	Enables users to configure Business Hours filters for group reports.

Table 13: Non Security-relevant User Rights

The user rights described in the following table should not be granted to Authorized Users in the evaluated configuration.

Name	Description and Reason for Restriction
Mobile Access	Enables users to access mobile web interface. The Mobile interface is excluded from the scope of the evaluation.
Access WhatsUp Gold Console	Enables users to access the WhatsUp Gold Admin Console application (nmconsole.exe) when FIPS 140-2 is enabled. Use of the Admin Console in the evaluated configuration is restricted to installation and initial configuration of the TOE, and to performance of database maintenance activities.
Access Tools	Enables users to access the WhatsUp Gold tools and utilities, enabling users to perform ping, traceroute, DNS lookup, MIB walker, Layer 2 Trace, and other operations on any device that is accessible on the network.

Name	Description and Reason for Restriction
System Administration	Enables users to edit system configuration items, including the maximum number of passive monitor records, maximum dimension of maps, and enabling and disabling mobile access. Setting these values should occur only during initial configuration.

Table 14: User Rights to be Restricted in the Evaluated Configuration

The TOE provides the following security management capabilities:

- Management of user accounts, including user passwords
- Manage Credentials Library
- Manage global email settings
- Manage LDAP credentials
- Perform a discovery scan of the network
- Manage alerts and notification policies
- Enable/disable Device Access Control Rights
- Manage Access Control Lists
- Manage Alert Center Threshold items
- Manage wireless devices
- Manage virtual devices
- Manage APM application profiles and instances
- Manage Dashboards.

6.1.5.2 Managing User Accounts

The TOE defines two default user accounts associated with the web GUI:

- **Administrator**—this Authorized User account has all user rights, including **Manage Users**, which grants the right to create and edit user accounts. The Administrator account is also given all group access rights, so that when enabled, this account is able to view and edit devices in all device groups
- **Guest**—the Guest account allows users to view the TOE without being able to modify any settings. By default, all user rights and all group access rights are disabled for this account. However, any user with the **Manage Users** right (including the Administrator account) can modify the Guest account rights. The Guest account is required to be deleted in the evaluated configuration.

Authorized Users with the **Manage Users** right can create additional user accounts as needed and manage existing user accounts. When initially created, a user account has no user rights assigned. As part of account creation and management, the Authorized User assigns user rights to the account, assigns the account to any user groups it is to be a member of, and sets the account password. Authorized Users require the **Change Your Password** user right in order to be able to change their own password.

6.1.5.3 Managing Credentials Library

The TOE's Credentials Library stores the applicable login, community string, or connection string information for various applications that the TOE can interact with, as follows:

- Windows (WMI Active Monitors, WMI Performance Monitors, and the Web Task Manager)
- SNMP v1, 2, and 3 devices in the TOE database
- ADO database

- VMware
- Telnet
- SSH.

Credentials are configured in the Credentials Library and used in several places throughout the TOE. Authorized Users with the **Configure Credentials** user right can manage the credentials used by the TOE.

A device needs SNMP credentials applied to it in order for SNMP-based active monitors to work. Similarly, NT Service Checks must have Windows credentials applied, and TOE database monitors require ADO connection information. VMware vCenter, and ESXi devices require VMware credentials to access system performance counters. The WhatsConfigured plug-in requires either an SSH or Telnet connection to gather configuration data and to perform various task scripts.

Managing Global Email Settings

The TOE provides Authorized Users with the **Email Settings** user right the ability to configure global email settings, which specify the settings for sending email notifications for various events that occur in the TOE, such as discovery of new devices and changes in the status of monitored devices.

6.1.5.4 Managing LDAP Credentials

The TOE provides Authorized Users with the **Configure LDAP Credentials** user right the ability to configure the credentials (connection data) the TOE uses to connect with an LDAP or AD authentication server in the operational environment.

6.1.5.5 Performing Discovery Scans

The details of how the TOE performs a network discovery are described in Section 6.1.7. Authorized Users with the **Access Discovery Console** user right are able to perform a network discovery.

6.1.5.6 Managing Alerts and Notifications

The details of the capabilities of alerts and notifications are described in Section 6.1.7. Authorized Users with the **Configure Alert Center** user right are able to create, edit, and delete Alert Center thresholds and notification policies.

6.1.5.7 Managing Alert Center Threshold Items

The details of the capabilities of thresholds are described in Section 6.1.7. When a monitored device property begins to operate outside of the defined threshold, it appears as an item in a dashboard report. Authorized Users with the **Manage Alert Center Threshold Items** user right are able to modify threshold items to indicate that the issue is known about (‘Acknowledge’) or that steps have been taken to address the issue (‘Resolve’).

6.1.5.8 Managing Wireless Devices

The TOE provides three methods for managing wireless devices; each method provides different management operations. Standard device management for wireless devices is performed via the Devices list using the ‘Manage Devices’ user right as described in Section 6.1.3. Wireless-specific device monitoring is performed via the Wireless tab using the ‘Access Wireless’ user right as described in Section 6.1.3. Global wireless settings are managed via the App Settings tab as described below

Authorized Users with the **Configure Wireless** user right are able to modify global wireless settings via the App Settings tab. The ‘Configure Wireless’ user right allows the authorized users to set wireless thresholds, set the wireless polling interval, set wireless data collection retention parameters, and manage wireless groups.

6.1.5.9 Managing Virtual Devices

The TOE provides two methods for managing virtual devices; each method provides different management operations. Standard device management for virtual devices is performed via the Devices list using the ‘Manage Devices’ user right as described in Section 6.1.3. Virtual-specific device management is performed via the Virtual tab as described below.

The TOE provides capabilities for monitoring and performing actions on virtual devices[6]. Authorized Users with the **Access Virtualization Actions Menu** user right are able to perform VM actions (power-on, power-off, suspend, reset, guest shutdown, guest restart, etc) on virtual devices. These actions are available both from the Virtual Map and from the Devices list.

The TOE provides the ability to query virtual devices via the Virtual Map. Authorized Users with the **Access WhatsVirtual Map** user right are able to list the virtual devices and view statistics for each virtual device accessed via the Virtual Map. This user right does not provide access to the underlying virtual host.

The TOE provides the ability to view virtual device reports in the Event Log accessed via the Virtual tab. Authorized Users with the **Access WhatsVirtual** user right are able to view virtual device reports. Authorized users without this user right are allowed to view the shell of the report, but cannot view the content of the report.

6.1.5.10 Managing Access Control Lists

The details regarding access control lists are provided in Section 6.1.3. Authorized Users with the **Manage Users** user right are able to manage access control lists.

6.1.5.11 Managing APM Application Profiles and Instances

Authorized Users with the **Access APM** user right are able to view and access the APM workspace. Authorized users must have the **Access APM** user right in addition to the corresponding **Configure APM Application Profiles** user right in order to create, edit, copy, and delete APM application profiles. Authorized users must have the **Access APM** user right in addition to the corresponding **Configure APM Application Instances** user right in order to create, edit, copy, and delete APM application instances. Additional details on managing APM application profiles and instances are provided in Section 6.1.3.2.

6.1.5.12 Managing Dashboards

The TOE provides the ability to copy dashboard views into another user's dashboard. Authorized users with the **Manage Users** security management user right and **Manage Dashboard View** access control user right are able to copy dashboards to other users. To copy a dashboard into another user's view, the Authorized User must have the **Manage Dashboard View** user right to perform a copy and the **Manage Users** user right to copy the dashboard view into another user's dashboard.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1(2): The TOE restricts to Authorized Users with the **Access Discovery Console** user right the ability to manage the behavior of network discovery scans.
- FMT_MTD.1(*): The TOE restricts to Authorized Users with the appropriate user rights the ability to manage TSF data and configurations.
- FMT_SMF.1: The TOE provides the security management capabilities necessary to manage the security functions of the TOE.
- FMT_SMR.1: The TOE defines a set of user rights that can be associated with Authorized Users to grant specific security management capabilities to Authorized Users.

6.1.6 Fault Tolerance

The TOE provides the capability, through the WhatsUp Gold Failover Manager application, to determine if the TOE has entered a failed state and to subsequently recover the TOE to a fully operational state. The failover mechanism provides the capability to automatically switch from a primary installation of WhatsUp Gold to a standby WhatsUp system (i.e., a second installation of WhatsUp Gold on a separate server) when the primary system is not functioning normally. The TOE can be configured to provide failover in the event all its services are disabled, or if any specified services are disabled. Use of the Failover Manager is optional in the evaluated configuration.

[6] A virtual device is a system virtual machine executing within a virtual environment. The virtual device executes on a virtual host (i.e., VMware) that is the physical system.

The TOE supports two possible configurations for failover support (identified in the TOE documentation as ‘scenarios’). In Scenario 1, the primary system’s database is located remotely on the secondary system. The primary system is responsible for running WhatsUp Gold and monitoring the network day-to-day. The secondary system is placed on standby, and in the event that the primary system goes down, takes over WhatsUp Gold duties for the network. Since it is hosting the primary system’s database, it has immediate access to the database. In Scenario 2, the primary and secondary systems both use a remote database, installed on a third server. The specific scenario is configured during installation. Note that neither scenario supports data redundancy. As a consequence, the guidance documentation recommends scheduling regular backups of the WhatsUp Gold database.

In situations where Failover Manager is not used, all WhatsUp Gold Premium services are set to automatically start after installation and activation. When WhatsUp Gold Failover Manager is installed and configured, all services except for the Failover Service (nmfailover.exe) are set to be manually started. The Failover Service is set to automatically start because it is the mechanism responsible for setting the active machine in the Failover deployment. When the Failover Service sets a machine to active, it manually turns on the services specified during configuration as necessary for the machine to successfully poll and manage the network. The Failover Service monitors the services running on the primary WhatsUp Gold machine. If any of the services included in the Failover Service fails unexpectedly, the primary machine is considered to be in a failed state and Failover is initiated.

During initial configuration, the Administrative user configures the services to be monitored for failover using the Failover Console available from the Tools menu of the WhatsUp Gold Console.

When enabled the Fault Tolerance function is designed to satisfy the following security functional requirements:

- FRU_FLT.2: The TOE provides the capability to fully restore all of the TOE’s capabilities in the event specified TOE services have failed.
- FPT_FLS.1: By providing a fully redundant backup for the primary TOE machine, the TOE is able to continue operating securely in the event the specified TOE services fail.

If Fault Tolerance is not enabled FRU_FLT.2 and FPT_FLS.1 are vacuously satisfied.

6.1.7 Network Monitoring

The TOE provides the capabilities to discover network devices, monitor the status of network devices, generate alerts about a monitored network device’s status, discover and monitor applications, and perform actions in response to changes in a monitored network device’s status.

6.1.7.1 Network Discovery Scan

The network discovery scan is the process the TOE uses to identify devices on the network that are to be monitored. This process scans each device to determine its manufacturer, model, and running software and services. The TOE uses this information to automatically assign commonly used monitors to each device.

Before the TOE can discover devices on a network, the administrative user needs to prepare both the devices and the TOE so that devices are discovered properly. In order for the TOE to properly discover and identify a device, the device must respond to requests the TOE uses during discovery—ping (ICMP) or open TCP port requests.

After the TOE discovers a device on an IP address, it queries the device to determine its manufacturer and model, components (such as fans, CPUs, and hard disks), operating system, and specific services (such as HTTP or DNS). To gain this information, the TOE uses a combination of SNMP, WMI, and VMware API. Therefore, devices from which such information is to be collected need to be configured to respond to SNMP or WMI requests and virtual network devices must be configured to respond to VMware vSphere API requests. The discovery process uses SNMP, WMI and VMware credentials to correctly identify devices and these need to be configured on the TOE before starting a discovery scan.

The TOE provides four methods for scanning the network:

- SNMP Smart Scan—the TOE discovers devices by reading SNMP information on the network. This method uses one or more SNMP-enabled devices to identify devices and sub-networks on the network.
- IP Range Scan—the TOE scans a range of IP addresses specified by the administrative user.

- Hosts File Scan—the TOE imports devices from a hosts file.
- VMware Scan—the TOE connects to VMware servers and uses the VMware vSphere API to gather information about the virtual environment. This scan uses a list of administrator-provided VMware vCenter servers or VMware hosts as targets for the scan.

When the TOE discovers devices, it tries to determine the type of each device so that it can monitor them appropriately. To determine a device type, the TOE compares the discovered attributes of each device to a set of criteria called device roles. Device roles do two things:

- Specify the criteria that a device must match to be identified as the device role.
- Specify the monitoring configuration that is applied to the device when it is added to the TOE.

The TOE provides a number of pre-configured device roles that are used to identify most common network devices. If the network includes devices that are not identified by the pre-configured set, the administrative user can create custom device roles during the initial configuration using the Discovery Console. Creating custom device roles is outside the evaluated configuration. The TOE does provide the ability to manage the assignment of devices roles to a device managed by the TOE.

The discovery process allows the Authorized User to associate action policies with device roles. Action policies describe what actions should be taken when a device's status changes. To use action policies during discovery, the Authorized User must configure them in the TOE before starting a discovery session, and then associate them with a device role.

The Authorized User can schedule discovery to run periodically. Each time discovery runs, it detects new devices on the network and suggests adding monitors on devices that have changed since the last discovery.

The TOE also provides capabilities to add devices to the monitoring network manually.

6.1.7.2 Device Groups

After the TOE discovers and identifies the role of a device, the Authorized User can add the device to a device group. Device groups allow the Authorized User to organize the devices discovered on the network to assist monitoring and management. There are three types of device group:

- Non-dynamic groups—also just referred to as "device groups". Each time devices are discovered on the network, a new device group is created containing devices discovered in the scan that are to be monitored. The TOE gives the new group a default name composed of the type of scan performed and a date-time stamp of when the scan took place (e.g., "SNMPScan (2011-04-07 10:24:37)").
- Dynamic groups—these are created by using SQL queries that search for devices based on administrator-specified criteria. By default, all devices discovered on the network are placed into a dynamic group called 'All devices'.
- Layer-2 group – allows devices to be mapped or grouped based on Layer-2 of the TCP/IP stack. Groups can be defined based on criteria so that when the map is updated, any new devices matching the criteria appear on the map.

The TOE provides Authorized Users with capabilities to manage non-dynamic, dynamic, and Layer-2 groups. Note that dynamic groups do not follow group access rights. Anyone with the ability to view the device group that a dynamic group is in can access that dynamic group. However, only devices that the user has the permission to view appear in the group.

After discovered devices are added to a device group, the TOE begins monitoring them immediately.

6.1.7.3 Monitors

The TOE provides the following types of monitors that are available for all device types:

- Active Monitors—monitor the state of device entities, such as processes, ports, services (e.g., device services, such as Web or email servers). Active monitors regularly query or poll the device services for which they are configured and wait for responses. If a query is returned with an expected response, the queried service is considered “up”. If a response is not received, or if the response is not expected, the queried service is considered “down” and a state change is issued on the device. The TOE includes a number of pre-configured Active Monitors in its Active Monitor Library. The full list is provided in the “Using Active Monitors” portion of the WhatsUp Gold Online Help.

- Passive Monitors—listen for device events. While active monitors actively query or poll devices for data, passive monitors passively listen for device events. The TOE supports three different types of passive monitor that can be configured and enabled for individual devices: SNMP Trap; Syslog; and Windows Event Log. Each type of monitor has associated with it a listener that must be configured on the TOE. When a listener collects an event (an SNMP Trap, a Syslog event, or a Windows Event Log event, as appropriate), it generates a record of the event and writes it to the appropriate TOE log (SNMP Trap Log, Syslog, Windows Event Log). The contents of each such record include: the date and time the event was detected by the TOE; the source of the event; and any information recorded in the event by its source.
- Performance Monitors—gather data about several performance components of the devices running on the network. The data can then be used to create reports that trend utilization and availability of these device components. The TOE provides performance monitors for the following characteristics:
    - CPU utilization—the percentage utilization of a monitored CPU
    - Disk utilization—the percentage utilization (i.e., how full) of a monitored hard disk
    - Interface utilization—the percentage utilization and throughput of a monitored device interface
    - Memory utilization—the percentage utilization of a monitored device’s memory
    - Ping latency and availability—these are measures of network performance and response time, based on the time taken for ICMP “ping” packets to traverse a network connection and the rate of lost packets.

  The TOE also provides the capability to create configurable performance monitors for the following items:

    - APC UPS—collects statistical output power usage information.
    - Printer—collects performance information from printers that support the Standard Printer MIB.
    - SNMP—collects values from selected SNMP performance counters (identified by OID and instance) available on a specified network device.
    - WMI performance counters—collects values from selected WMI counters available on a specified network device.
    - Active Script—allows the Authorized User to write VBScript or Jscript to poll one or more SNMP or WMI values, perform math or other operations on those values, and graph a single output value. The capabilities of Active Script performance monitors have not been assessed as part of the evaluation.
    - SSH—allows the Authorized User to specify a command to be run on the remote device, such as a Unix command or a Perl script. The command or script must return a single numeric value. The monitor will connect to the device using SSH in order to execute the command. The capabilities of SSH performance monitors have not been assessed as part of the evaluation.

  The performance monitor reports the TOE generates include the date and time range over which the performance data was collected, the identity of each device from which performance data was collected, and the specific performance data collected from each identified device.

- Flow Monitors (provided by the WhatsUp Gold Flow Monitor plug-in)—use Cisco NetFlow, sFlow, J-Flow and IPFIX data from switches, routers, and Adaptive Security Appliances (ASA) to gather, analyze, report, and alert on LAN/WAN traffic patterns and bandwidth utilization. As a minimum, the TOE collects: the identity of the interfaces through which traffic flows; network protocol (such as TCP or UDP); source identifier (host name or IP address); and destination identifier (host name or IP address). The TOE can generate reports of flow-related data for individual interfaces that include the sender, receiver, and protocol.

6.1.7.4 Application Discovery and Monitoring

The Application discovery and monitoring feature enables the TOE to discover and monitor applications. From the perspective of the TOE, an application is made up of one or more "components" running on one or more monitored devices. A component is a single data point that is collected as part of an application profile. Components can be processes, services, scripts, and system statistics. The component of an application profile can be another application, supporting nesting of applications. The following components are available for use in the TOE:

- CPU Utilization
- Database Query - MySQL, Oracle, SQL Server
- Disk Utilization
- Memory Utilization -Physical, Virtual
- Network Port Checks -Custom, Echo, FTP, HTTP, HTTPS, IMAP4, NNTP, POP3, Radius, SMTP, Time
- Process Check - SNMP, WMI
- Scripting - JavaScript, PowerShell, VBScript
- Service Check - SNMP, WMI
- SNMP
- SSH - Active, Performance
- WMI - Formatted, Raw

Before the TOE can discover and monitor applications, the TOE must have completed a network discovery scan. Application discovery does not occur automatically. Authorized users must manually initiate a scan of the monitored network devices, searching for applications that comply with the application profile. To be discoverable, an application must have at least one discoverable service or process component associated with its application profile. The application discovery feature scans for processes and services on the network device, as defined in the application profiles. In order for the TOE to properly discover an application, the device must respond to requests the TOE uses during discovery—WMI or SNMP requests.

The TOE monitors application status based on components. In order to monitor an application, it is first necessary to create an application profile or use a predefined application profile. An application profile defines a collection of individual components that are used to monitor the application. These components are used by an application instance to reflect the health and status of the application. An application instance is created from the application profile by associating it with the actual devices that host the components of the application as defined by the application profile. An application instance is a running copy of an application profile that monitors the defined collection of components and distinct applications. The TOE allows the Authorized User to create custom application profiles.

Application types group application profiles, instances, and components by the type of application (e.g., SQL Server, IIS, Windows 2008 Server) to ease in administration. Each application profile belongs to one application type.

The TOE defines three categories of applications:

- Simple application—an application that is not dependent on another application to run (e.g., Microsoft Server 2008 R2).
- Complex application—an application configured to be dependent on one or more applications to run (e,g., WhatsUp Gold requires IIS and SQL Server).
- Discrete application—an application upon which a complex application has a dependency. In the example above, IIS and SQL Server are discrete applications on which the complex application WhatsUp Gold is dependent.

6.1.7.5 Actions and Alerts

Actions are designed to perform a task when a device, application, or monitor state change occurs.

The Authorized User configures an action to perform a specified task. Actions can try to correct the problem, notify someone of the state change, or launch an external application. The Authorized User can assign the action to a device, application, or to an active or passive monitor. Note, the evaluation does not cover the efficacy of any actions in actually correcting problems, only that the TOE invokes actions as configured. Additionally, where the action is for the TOE to generate and send a notification, the TOE relies on the appropriate handler in the operational environment (e.g., SMTP server) to deliver the notification to its intended destination.

When assigned to an active monitor, actions fire according to the state changes the monitor issues. For example, the Authorized User can configure an Email Action to send an email alert when the active monitor for a Web server issues a down state change.

The Authorized User can configure actions on a single device or monitor, or define an Action Policy to use across multiple devices or monitors. The TOE also supports Recurring Actions, which provide the ability to fire actions based on a regular schedule (e.g., daily, weekly, every *x* minutes) independent of the status of devices.

The TOE's Alert Center capability handles alerting on performance monitors, passive monitors, flow monitors, and the TOE's system health using the following mechanisms:

- Thresholds—these are the benchmark mechanisms Alert Center uses to check against the database. If the TOE finds that an aspect has exceeded or fallen below the parameters set in a threshold, it is considered out of threshold. These out of threshold aspects are logged as items in the Alert Center Items report. Each item contains the following information:

    - **Item**—the device that has gone out of the parameters of the selected threshold(s).
    - **Threshold**—the specific threshold for which the item was created.
    - **Aspect**—the device aspect that has gone out of the parameters of the threshold.
    - **Value**—the value that caused the device aspect to fall out of threshold.
    - **Date/Time**—the date and time Alert Center found the device aspect out of threshold and created the item.

  The Authorized User can find data for Alert Center items on the Alert Center Home page and in Alert Center reports

- Notification Policies—when an aspect goes out of threshold and is logged as an item, associated notification policies begin sending notifications to alert administrative users of the problem. These policies can include multiple steps that begin at administrator-specified intervals to notify multiple people of persisting problems. After a problem is fixed, administrative users can be notified of the fix and subsequent steps of a running notification policy can be stopped. The TOE supports email and SMS-based notifications.

APM allows the administrator to configure action policies that can be applied to application instances and components being monitored. An action policy defines the actions to take when an application instance or component transitions from one state to another. Application and components can be in the following states: Up, Down, Warning, Unknown, and Maintenance. State transition rules evaluate whether to permit the associated action to fire based on the amount of time the source was in a previous state. The action rules determine which action to fire, how long to wait in the target state before firing the action, and which blackout policy to apply. The blackout policy prohibits an action from firing during defined periods of time when activities such as server maintenance generate large numbers of actions that are not of interest. After APM actions, action policies, and blackout policies are created, you can assign an action policy to an application instance or component.

6.1.7.6 Dashboards and Reports

A Dashboard is an administrator-specific, configurable reports display. A Dashboard contains multiple views that let the Authorized User organize various reports by the type of information they display.

The TOE provides the following Dashboard types:

- Home—can display both Home- and Device-level dashboard reports. The Authorized User can place any dashboard report on a Home dashboard, mixing and matching summary, group, and device-specific data.

- Device status—limited to display only Device-level dashboard reports. Only dashboard reports specific to a single device can be placed on a device dashboard. When the device-in-context is changed, the reports displayed show data corresponding to the newly selected device.
- Top 10—displays Top 10 full reports for network devices.

Each of the dashboard types supports multiple administrator-defined views and up to 15 small reports known as dashboard reports can be displayed within each view. These dashboard reports show content ranging from Current Interface and CPU utilization to Syslog messages. The TOE provides capabilities to manage dashboards and dashboard views.

The TOE supports two general types of report:

- Dashboard Reports—the TOE offers over 100 configurable dashboard reports for display in dashboard views. These smaller reports show similar information to that found in the full reports. Because of their smaller size, multiple reports can be placed in a dashboard view, making it possible to view multiple reports simultaneously. Dashboard reports can be Device dashboard or Home dashboard reports, depending on the dashboard type in which they can be displayed. Dashboard reports are also broken down into categories depending on the type of information they display:
    - **Alert Center**—display information that pertains to device thresholds and threshold summary information
    - **CPU Utilization—**display information that pertains to device and network CPU levels
    - **Custom Performance Monitors**—display information that pertains to custom performance monitors created by the Authorized User
    - **Disk Utilization**—display information that pertains to device and network disk capacity levels
    - **Flow Monitor—**display data from Flow Monitor and can be used within Flow Monitor report views as well as dashboard views
    - **General**—display information on your TOE settings and diagnostics, database size, as well as device-specific and administrator-configured details
    - **Interface Errors and Discards**—display information that pertains to device interface data errors and data discards
    - **Interface Utilization—**display information that pertains to device and network interfaces
    - **Inventory**—provide a break-down of network devices and their settings, including Actions, monitors, and policies
    - **Memory Utilization**—display information that pertains to device and network memory levels
    - **Performance (Historic and Last Poll)**—display information gathered from WMI and SNMP Performance Monitors regarding your network devices' CPU, disk, interface, and memory utilization; and ping latency and availability
    - **Ping Availability and Response Time**—display information that pertains to device ping availability, response time, and packet loss
    - **Problem Areas**—trouble-shooting dashboard reports that advise the Authorized User of network issues
    - **Split Second Graphs**—real-time graphs that display information on SNMP and WMI performance counters. These reports allow the Authorized User to include the real-time information available on the Web Performance Monitor network tool and the Web Task Manager network tool in any dashboard view
    - **Threshold**—display information on the network's CPU, disk, interface, memory utilization, and ping function at or above a specific threshold

    - **Top 10**—display the top devices on the network according to their CPU, disk, interface, memory utilization, and ping function
    - **Virtualization**—display information about vCenter servers, virtual hosts and their associated virtual machines, including details about the virtual host or vCenter server, a list of the virtual machines, as well as CPU, disk, interface, and memory utilization for virtual machines.
    - **Wireless**—display information about Wireless Access Point (WAP) devices and the devices connected to the WAPs, transmit and receive errors, and syslog messages.
- Full Reports—used to troubleshoot and monitor performance and historical data that has been collected during the operation of the TOE. Full reports are broken down by the scope and the type of information displayed within each report. There are three categories for full reports based on the scope of information displayed:
    - System—display system-wide information. System reports do not focus on a particular device nor a specific device group. For example, the General Error Log and the Web User Activity Log are system reports.
    - Group—display information relating to a specific device group. For example, the Group State Change Timeline and the Group Actions Applied reports are group reports.
    - Device—display information relating to a specific device. For example, the Device Status Report is a device report.

  There are three categories for full reports based on the type of information displayed:

    - Performance—display information gathered from WMI and SNMP Performance Monitors regarding network devices' CPU, disk, interface, and memory utilization, and ping latency and availability. For example, the Device Custom Performance Monitors and the Group Memory Utilization reports are performance reports.
    - Problem Areas—troubleshooting reports that allow the Authorized User to investigate network issues. For example, the Group Active Monitor Outage and the Passive Monitor Error Log are problem area reports.
    - General—display information on TOE settings and diagnostics, as well as device-specific and user-configured details. For example, the Home, Top 10, and Device Status dashboards/full reports are general reports.

The Network Monitoring function is designed to satisfy the following security functional requirements:

- FNM_DSC_(EXT).1: The TOE provides the capability to scan a network for devices using ICMP and TCP open port.
- FNM_DSC_(EXT).2: The TOE provides the capability to query network devices it has discovered using SNMP and WMI, in order to obtain information such as manufacturer, model, components, operating system, and services.
- FNM_DSC_(EXT).3: The TOE provides the capability to scan monitored network devices for applications using application profiles as the criteria for the scan.
- FNM_MNT_(EXT).1: The TOE supports the following types of monitor for monitoring discovered network devices and the network itself: active; passive; performance; and flow.
- FNM_MNT_(EXT).2: The active monitor capability of the TOE is able to query devices on the network for the following services: DNS; Windows Service; TCP/IP Service; Telnet; SMTP; FTP; HTTP; and SQL Server. The TOE can report on the status of the service based on the response it receives to its query.
- FNM_MNT_(EXT).3: The passive monitor capability of the TOE is able to detect and record the following types of event generated by devices on the network: SNMP trap; syslog message; and Windows Event Log events.

- FNM_MNT_(EXT).4: The performance monitor capability of the TOE is able to collect and report on the following performance-related data from devices on the network: CPU utilization; disk utilization; interface utilization, memory utilization; ping latency and availability; statistical output power usage, printer, SNMP performance counters, WMI performance counters.
- FNM_MNT_(EXT).5: The flow monitor capability of the TOE is able to collect and report on flow data produced by NetFlow, sFlow, Jflow and IPFIX protocols.
- FNM_ACT_(EXT).1: The TOE can associate actions with devices, active monitors, passive monitors, and applications and perform actions when criteria to trigger the action are satisfied.
- FNM_ACT_(EXT).2: The TOE can associate alerts with performance monitors, passive monitors and flow monitors, and can generate a log when an alerting threshold has been exceeded.
- FNM_ACT_(EXT).3: The TOE can associate notification policies with alerting thresholds and apply the notification policy when the alerting threshold is exceeded. The TOE supports email and SMS-based notifications.

7. Protection Profile Claims

There are no Protection Profile claims in this Security Target.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats and usage assumptions by the security objectives.

	T.ACCESS	T.AUTHORITY	T.CONFIDENTIALITY	T.DEVICE_STATUS	T.FAILURE	T.UNACCOUNTABILITY	A.ADMIN	A.CREDEN	A.DEV_COMMS	A.HTTPS	A.INSTALL	A.MANAGE	A.PHYSICAL	A.RESPONSE	A.TOE_ONLY
O.ACCESS	X	X													
O.AUDIT						X									
O.I&A	X														
O.FAILOVER					X										
O.MANAGE		X													
O.MONITOR				X											
O.PROTECT			X												
O.ROLES		X													
OE.ADMIN							X								
OE.CERTIFICATES			X												
OE.CREDEN								X							
OE.DB			X												
OE.DEV_COMMS									X						
OE.HTTPS										X					
OE.INSTALL	X					X					X				
OE.MANAGE						X						X			
OE.PHYSICAL	X												X		
OE.RESPONSE														X	
OE.TIME						X									
OE.TOE_ONLY	X														X

Table 15: Environment to Objective Correspondence

8.1.1.1 T.ACCESS

Unauthorized entities may be able to gain logical access to the TOE and its data.

This threat is countered by the following security objectives:

- O.I&A—addresses this threat by ensuring that Authorized Users are identified and authenticated before gaining access to the capabilities of the TOE.
- O.ACCESS—addresses this threat by ensuring that Authorized Users are restricted in how they can access controlled objects (which provide the internal representations of discovered and monitored network devices), based on user privileges and object access rights.
- OE.PHYSICAL—supports addressing this threat by ensuring the computers on which the TOE is installed are located in physically secure areas such that access is restricted to authorized administrative users of the TOE. This ensures that those users that access the TOE console are authorized to access all the capabilities of the TOE.
- OE.INSTALL—supports addressing this threat by ensuring the TOE is installed on an operating system that provides the capabilities to protect the TOE from tampering or bypass.
- OE.TOE_ONLY—supports addressing this threat by ensuring that the computer system(s) on which the TOE components are installed are dedicated to the function of the TOE, so that no applications will exist on those systems that might attempt to gain unauthenticated access to the TOE (e.g., by invoking its console application).

8.1.1.2 T.AUTHORITY

Authorized Users may be able to perform actions for which they do not have authorization.

This threat is countered by the following security objectives:

- O.ACCESS—addresses this threat by ensuring the TOE enforces a role-based access control policy on the objects it controls.
- O.MANAGE—addresses this threat by ensuring the management capabilities of the TOE are restricted based on the authorizations granted to Authorized Users.
- O.ROLES—supports addressing this threat by associating Authorized Users with administrative privileges that determine their access control authorizations within the TOE.

8.1.1.3 T.CONFIDENTIALITY

An attacker may be able to observe TSF data that is stored in the IT environment or communicated to devices on the network.

This threat is countered by the following security objectives:

- O.PROTECT—addresses this threat by ensuring the TOE provides mechanisms that can protect the confidentiality of authentication credentials stored in the IT environment, communications with devices on the network, and communications with the LDAP or AD server.
- OE.CERTIFICATES—the operational environment supports the TOE in countering this threat by providing a means by which public key certificates can be created and managed. The TOE uses these certificates to support key exchange and authenticate parties at either end of an encrypted communication.
- OE.DB—the operational environment supports the TOE in countering this threat by protecting the TSF data stored in the DB so that only the TOE can access the data.

8.1.1.4 T.DEVICE_STATUS

The status of network devices may change, to the detriment of network operations, without the knowledge of network administrators.

This threat is countered by the following security objective:

- O.MONITOR—addresses this threat by ensuring the TOE provides capabilities to discover network devices, monitor the status of network devices, generate alerts about a monitored network device's status, and perform actions in response to changes in a monitored network device's status.

8.1.1.5 T.FAILURE

The capabilities of the TOE may become unavailable in the event one or more of its services fails.

This threat is countered by the following security objective:

- O.FAILOVER—addresses this threat by ensuring the TOE provides capabilities to monitor its services and to be able to failover to a backup system in the event it detects a failure of its monitored services. This in turn ensures the capabilities of the TOE do not become unavailable due to a failure of a TOE service.

8.1.1.6 T.UNACCOUNTABILITY

The authorized users of the TOE may not be held accountable for their actions within the TOE, resulting in unauthorized and undetected activities that compromise the TOE or the data it protects.

This threat is countered by the following security objectives:

- O.AUDIT—addresses this threat by providing the audit mechanism to record the actions of a specific user, and to review the audit trail based on the identity of the user.
- OE.TIME—supports addressing this threat by ensuring the operational environment provides a reliable timestamp the TOE can use in generating audit records.
- OE.INSTALL—supports addressing this threat by providing logical protection of the audit records stored in the operational environment.
- OE.MANAGE—supports addressing this threat by ensuring those managing the TOE are competent to do so. One of the tasks expected of a competent manager of the TOE would be to ensure the space available for storing the audit trail is not exhausted.

8.1.1.7 A.ADMIN

The administrative users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

This assumption is covered by the following security objective for the operational environment:

- OE.ADMIN—this objective ensures the administrative users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

8.1.1.8 A.CREDEN

Users granted authorization to logon to the TOE shall choose passwords that satisfy complexity requirements as specified in the guidance documentation.

This assumption is covered by the following security objective for the operational environment:

- OE.CREDEN—this objective ensures the users granted authorization to logon to the TOE choose passwords that satisfy the complexity requirements specified in the guidance documentation.

8.1.1.9 A.DEV_COMMS

The TOE and each device it monitors will be configured to use the most secure method of communication permitted by the particular device.

This assumption is covered by the following security objective for the operational environment:

- OE.DEV_COMMS—this objective ensures the TOE and each device it monitors are configured to use the most secure communication method permitted by the particular device.

8.1.1.10 A.HTTPS

The TOE will be configured so as to require the use of HTTPS to access its web-based management GUI.

This assumption is covered by the following security objective for the operational environment:

- OE.HTTPS—this objective ensures the TOE is configured to require the use of HTTPS in order to access its web-based management GUI.

8.1.1.11 A.INSTALL

The TOE will be installed within the context of operating systems that provide the logical protection necessary to ensure the TOE cannot be tampered with or bypassed.

This assumption is covered by the following security objective for the operational environment:

- OE.INSTALL—this objective ensures the TOE is installed within the context of operating systems that provide the logical protection necessary to ensure the TOE cannot be tampered with or bypassed.

8.1.1.12 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is covered by the following security objective for the operational environment:

- OE.MANAGE—this objective ensures there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.

8.1.1.13 A.PHYSICAL

The computers on which the TOE is installed are located in physically secure areas such that access is restricted to authorized administrative users of the TOE.

This assumption is covered by the following security objective for the operational environment:

- OE.PHYSICAL—this objective ensures the computers on which the TOE is installed are located in physically secure areas such that access is restricted to authorized administrative users of the TOE.

8.1.1.14 A.RESPONSE

Network devices to be monitored by the TOE are configured to respond to ping or open TCP port requests.

This assumption is covered by the following security objective for the operational environment:

- OE.RESPONSE—this objective ensures the network devices to be monitored by the TOE are configured to respond to ping or open TCP port requests.

8.1.1.15 A.TOE_ONLY

The computing system(s) on which the components of the TOE are installed are dedicated to its function and are not used for any other purpose.

This assumption is covered by the following security objective for the operational environment:

- OE.TOE_ONLY—this objective ensures the computing systems on which the TOE components are installed are dedicated to the TOE’s function.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the security requirements specified in the Security Target.

8.2.1 Security Functional Requirements Rationale

All security functional requirements identified in this Security Target are fully addressed in this section and each is mapped to the objective it is intended to satisfy. **Table 16** summarizes the correspondence of functional requirements to TOE security objectives.

	O.ACCESS	**O.AUDIT**	**O.FAILOVER**	**O.I&A**	**O.MANAGE**	**O.MONITOR**	**O.PROTECT**	**O.ROLES**
FAU_GEN.1		X						
FAU_GEN.2		X						
FAU_SAR.1		X						
FAU_SAR.2		X						
FAU_SAR.3		X						
FAU_STG.3		X						
FCS_CKM.1							X	
FCS_CKM.4							X	
FCS_COP.1(*)							X	
FDP_ACC.1	X							
FDP_ACF.1	X							X
FIA_ATD.1				X				X
FIA_UAU.2				X				
FIA_UAU.5				X				
FIA_UID.2				X				
FMT_MOF.1(*)					X			
FMT_MSA.1					X			
FMT_MSA.3					X			
FMT_MTD.1(*)					X			
FMT_SMF.1					X			
FMT_SMR.1								X
FNM_ DSC_(EXT).1						X		
FNM_DSC_(EXT).2						X		
FNM_DSC_(EXT).3						X		
FNM_MNT_(EXT).1						X		
FNM_MNT_(EXT).2						X		
FNM_MNT_(EXT).3						X		
FNM_MNT_(EXT).4						X		
FNM_MNT_(EXT).5						X		
FNM_ACT_(EXT).1						X		
FNM_ACT_(EXT).2						X		
FNM_ACT_(EXT).3						X		
FPT_FLS.1			X					
FRU_FLT.2			X					
FTA_SSL.4				X				

Table 16: Objective to Requirement Correspondence

8.2.1.1 O.ACCESS

The TOE shall restrict access of Authorized Users to controlled objects, based on user privileges and object access rights.

This TOE security objective is met by the following SFRs:

- FDP_ACC.1, FDP_ACF.1—these SFRs work together to specify the scope of the access control policy and the rules that enforce the access control policy within its defined scope, in order to control access to the TOE's objects.

8.2.1.2 O.AUDIT

The TOE shall be able to log the activities of Authorized Users and shall provide capabilities to review logged activities.

This TOE security objective is met by the following SFRs:

- FAU_GEN.1—defines the set of events that the TOE must be capable of recording. This requirement ensures that the TOE has the ability to audit the activities of authorized users. This requirement also defines the information that must be contained in the audit record for each auditable event.
- FAU_GEN.2—ensures that the audit records associate a user identity with the auditable event.
- FAU_SAR.1—provides the Authorized Users with the capability to read all audit data contained in the audit trail. This requirement also mandates the audit information be presented in a manner that is suitable for the Authorized Users to interpret the audit trail.
- FAU_SAR.2—supports the satisfaction of the security objective by ensuring only appropriately Authorized Users are able to review the contents of the audit trail.
- FAU_SAR.3—supports FAU_SAR.1 by providing the Authorized Users the ability to sort the audit records residing in the audit trail, thus assisting the Authorized Users in reviewing the activities occurring on the TOE.
- FAU_STG.3—supports FAU_GEN.1 by ensuring an Administrative User is notified if the space available for storing generated audit records drops below 10% of capacity. This enables the Administrative User to take appropriate actions to ensure the space available for storing audit records is not exhausted, and that no audit records are lost.

8.2.1.3 O.FAILOVER

The TOE shall provide the capability to failover to a backup system in the event of a failure of one or more of its services.

This TOE security objective is met by the following SFRs:

- FPT_FLS.1, FRU_FLT.2—these SFRs work together to ensure the capabilities of the TOE continue to be available in the event one or more TOE services, as configured by an Administrative User, fail, and the secure state of the TOE is preserved.

8.2.1.4 O.I&A

The TOE shall be able to identify and authenticate authorized users that access the TOE remotely.

This TOE Security Objective is met by the following SFRs:

- FIA_UAU.2—requires remote users to be successfully authenticated before the TSF will allow any other TSF-mediated actions to be performed on their behalf.
- FIA_UID.2—requires remote users to be successfully identified before the TSF will allow any other TSF-mediated actions to be performed on their behalf.

- FIA_UAU.5—requires that the TOE provide a local authentication mechanism and also be able to support an external authentication mechanism. These mechanisms are used by the TOE to authenticate the claimed identities of remote users.
- FIA_ATD.1—supports the other SFRs by defining the attributes of users, including an identifier that is used to by the TOE to determine a user's identity and authentication data that is to be presented by the user to authenticate their claimed identity to the TOE.
- FTA_SSL.4—supports the other SFRs by providing the capability for the user to terminate their interactive session with the TOE, thus contributing to the protection of the user's account from abuse.

8.2.1.5 O.MANAGE

The TOE shall provide capabilities to manage its security functions and shall restrict those capabilities to authorized users.

This TOE Security Objective is met by the following SFRs:

- FMT_SMF.1—requires the TOE to provide the functions and facilities necessary for the Authorized Users to manage the TOE.
- FMT_MOF.1(1)—supports FMT_SMF.1 by specifying how management of the access control function is to be restricted to defined roles.
- FMT_MOF.1(2)—supports FMT_SMF.1 by specifying how management of network discovery scans is to be restricted to defined roles.
- FMT_MSA.1—supports FMT_SMF.1 by specifying how management of the security attributes associated with enforcement of the access control policy are to be restricted to defined roles.
- FMT_MSA.3—supports FMT_SMF.1 by specifying how security attributes associated with enforcement of the access control policy are to be initialized, and what roles are able to specify alternative initial values for those attributes.
- FMT_MTD.1(all iterations)—supports FMT_SMF.1 by specifying how management of various TSF data items is to be restricted to defined roles.

8.2.1.6 O.MONITOR

The TOE shall provide capabilities to discover network devices, monitor the status of network devices, generate alerts about a monitored network device's status, and perform actions in response to changes in a monitored network device's status.

This TOE Security Objective is met by the following SFRs:

- FNM_DSC_(EXT).1—requires the TOE to provide the capabilities necessary to scan a network for devices to be monitored.
- FNM_DSC_(EXT).2—requires the TOE to provide the capabilities necessary to enable the TOE to query discovered network devices.
- FNM_DSC_(EXT).3—requires the TOE to provide the capabilities necessary to enable the TOE to scan monitored network devices for applications.
- FNM_MNT_(EXT).1, FNM_MNT_(EXT).2, FNM_MNT_(EXT).3, FNM_MNT_(EXT).4, FNM_MNT_(EXT).5—these requirements specify the monitoring mechanisms to be provided by the TOE and specific capabilities of different monitoring mechanisms.
- FNM_ACT_(EXT).1—requires the TOE to be able to perform actions on monitored network devices when triggered by events on the device.
- FNM_ACT_(EXT).2—requires the TOE to be able to generate logs of alerting thresholds associated with devices and device monitors when those thresholds are exceeded.

- FNM_ACT_(EXT).3—requires the TOE to be able to apply notification policies associated with alerting thresholds when those thresholds are exceeded.

8.2.1.7 O.PROTECT

The TOE shall provide mechanisms to protect the confidentiality of TSF authentication credentials stored in the IT environment, communications between itself and network devices, and communications with the LDAP or AD server.

This TOE Security Objective is met by the following SFRs:

- FCS_COP.1(all iterations)—require the TOE to provide cryptographic operations that support symmetric data encryption and decryption, digital signature services, cryptographic hashing, keyed-hash message authentication and key agreement services that can be used to protect the confidentiality of TSF data that is stored in the operational environment or communicated to external IT entities.
- FCS_CKM.1—supports FCS_COP.1 by requiring the TOE be able to generate the symmetric keys necessary for it to support its cryptographic functions.
- FCS_CKM.4—supports FCS_CKM.1 and FCS_COP.1 by requiring the TOE to destroy cryptographic keys.

8.2.1.8 O.ROLES

The TOE shall be able to associate Authorized Users of the TOE with the privileges that determine the access control and security management capabilities available to them.

This TOE Security Objective is met by the following SFRs:

- FMT_SMR.1—requires the TOE to define security management privileges that are associated with Authorized Users of the TOE.
- FDP_ACF.1—defines the access control policy and the User Rights required by an Authorized User to perform specific operations on specific controlled objects.
- FIA_ATD.1—supports FMT_SMR.1 and FDP_ACF.1 by associating User Rights with Authorized Users.

8.2.2 Security Assurance Requirements Rationale

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The TOE is targeted at an environment with good physical access security where it is assumed that attackers will have low attack potential. Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures. Therefore, the target assurance level of EAL 2 augmented with ALC_FLR.1 is appropriate for such an environment.

8.3 Requirement Dependency Rationale

The following table identifies the dependencies of the security functional requirements in this ST.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	**See rationale**
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.3	FAU_STG.1	**See rationale**
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4	FCS_COP.1(1), FCS_CKM.4
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1

ST Requirement	CC Dependencies	ST Dependencies
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	**See rationale**, FCS_CKM.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	**See rationale**
FCS_COP.1(5)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1(6)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1(7)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	FCS_CKM.1, FCS_CKM .4
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_ATD.1	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	none
FIA_UID.2	none	none
FMT_MOF.1(*)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1	(FDP_ACC.1 or FDP_IFC.1), FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1(*)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FNM_DSC_(EXT).1	none	none
FNM_DSC_(EXT).2	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_DSC_(EXT).3	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_MNT_(EXT).1	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_MNT_(EXT).2	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_MNT_(EXT).3	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_MNT_(EXT).4	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_MNT_(EXT).5	FNM_DSC_(EXT).1	FNM_DSC_(EXT).1
FNM_ACT_(EXT).1	FNM_DSC_(EXT).1, FNM_MNT_(EXT).1	FNM_DSC_(EXT).1, FNM_MNT_(EXT).1
FNM_ACT_(EXT).2	FNM_MNT_(EXT).1	FNM_MNT_(EXT).1
FNM_ACT_(EXT).3	FNM_ACT_(EXT).2	FNM_ACT_(EXT).2
FPT_FLS.1	none	none
FRU_FLT.2	FPT_FLS.1	FPT_FLS.1
FTA_SSL.4	none	none

Table 17: Requirement Dependencies

The following rationale justifies the CC-defined dependencies that are not satisfied by the ST requirements:

- FAU_GEN.1 dependency on FPT_STM.1: The TOE obtains the reliable timestamp for the audit records it generates from the underlying operating system. This is covered by OE.TIME.

- FAU_STG.3 dependency on FAU_STG.1. The TOE relies on the operational environment to protect stored audit records from unauthorized modification or deletion. This is covered by OE.PHYSICAL and OE.TOE_ONLY.
- FCS_COP.1(2) dependency on (FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1): The TOE obtains the keys necessary to support RSA cryptography from the operational environment, and leaves all aspects of key generation and certificate management up to the operational environment. This is covered by OE.CERTIFICATES.
- FCS_COP.1(4) dependency on (FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1): FCS_COP.1(4) specifies requirements for a cryptographic hash mechanism (i.e., SHA1), which does not require any cryptographic keys. Therefore, the dependency is not applicable.

8.4 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF.

	Security audit	**Cryptographic Support**	**User data protection**	**Identification and authentication**	**Security management**	**Fault Tolerance**	**Network monitoring**
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_STG.3	X						
FCS_CKM.1		X					
FCS_CKM.4		X					
FCS_COP.1(*)		X					
FDP_ACC.1			X				
FDP_ACF.1			X				
FIA_ATD.1				X			
FIA_UAU.2				X			
FIA_UAU.5				X			
FIA_UID.2				X			
FMT_MOF.1(*)					X		
FMT_MSA.1					X		
FMT_MSA.3					X		

	Security audit	Cryptographic Support	User data protection	Identification and authentication	Security management	Fault Tolerance	Network monitoring
FMT_MTD.1(*)					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_FLS.1						X	
FRU_FLT.2						X	
FTA_SSL.4				X			
FNM_DSC_(EXT).1							X
FNM_DSC_(EXT).2							X
FNM_DSC_(EXT).3							X
FNM_MNT_(EXT).1							X
FNM_MNT_(EXT).2							X
FNM_MNT_(EXT).3							X
FNM_MNT_(EXT).4							X
FNM_MNT_(EXT).5							X
FNM_ACT_(EXT).1							X
FNM_ACT_(EXT).2							X
FNM_ACT_(EXT).3							X

Table 18: Security Functions vs. Requirements Mapping

8.5 PP Claims Rationale

See Section 7, Protection Profile Claims.