National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Ipswitch, Inc.

for

WhatsUp Gold Premium with Plug-Ins Version 16.1.99

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2014-01-16

Validation Report Number: CCEVS-VR-VID10487-2014

CCTL: Leidos (formerly SAIC) Common Criteria Testing Laboratory

Assurance Level: EAL2 Augmented with ALC_FLR.1

Protection Profile Identifier: None

Original Signed By

Acting Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By

Information Assurance Director
National Security Agency

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

WhatsUp Gold Premium Version 16.1.99

Report Number: CCEVS-VR-VID10487-2014
Dated: 16 January 2014
Version: 2.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

The Aerospace Corporation
El Segundo, CA

Patrick Mallett

The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

Leidos, Incorporated (formerly SAIC)
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Ipswitch WhatsUp Gold Premium Version 16.1.99 product was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in January 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC_FLR.1. The information in this Validation Report derives largely from the Evaluation Technical Report (ETR) and associated test reports produced by the Leidos evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

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 product, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the WhatsUp Gold Premium Security Target (ST).

1.1 Evaluation Details

Table 1. Evaluation Details

Evaluated Product:	The Target of Evaluation (TOE) is WhatsUp Gold Premium with Plug-Ins Version 16.1.99
Sponsor:	**Ipswitch, Inc.** 83 Hartwell Avenue Lexington MA, 02421
Developer:	**Ipswitch, Inc.** 83 Hartwell Avenue Lexington MA, 02421
CCTL:	Leidos, Incorporated (formerly SAIC) 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	20 January 2012
Completion Date:	16 January 2014
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	EAL 2 augmented with ALC_FLR.1

Description: The WhatsUp Gold Premium with Plug-Ins Version 16.1.99 product 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. 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.

Disclaimer: The information contained in this Validation Report is not an endorsement of the WhatsUp Gold Premium 16.1.99 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

PP: None

Evaluation Personnel: *Leidos, Incorporated (formerly SAIC)*:

Katie Sykes
Chris Keenan
Dawn Campbell
Julie Cowan

Validation Body: National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operating environment are intended to counter:

- Unauthorized entities may be able to gain logical access to the TOE and its data.
- Authorized Users may be able to perform actions for which they do not have authorization.
- An attacker may be able to observe TSF data that is stored in the IT environment or communicated to devices on the network.
- The status of network devices may change, to the detriment of network operations, without the knowledge of network administrators.
- The capabilities of the TOE may become unavailable in the event one or more of its services fails.
- 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.

2 Identification

The evaluated product is **WhatsUp Gold Premium with Plug-Ins Version 16.1.99.**

3 Security Policy

The TOE enforces the following security policies as described in the ST:

Note: *Much of the description of the WhatsUp Gold Premium 16.1.99 security policy has been extracted and reworked from the WhatsUp Gold Premium Version 16.1.99 Security Target and Final ETR.*

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- The administrative users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- Users granted authorization to logon to the TOE shall choose passwords that satisfy complexity requirements as specified in the guidance documentation.

- The TOE and each device it monitors will be configured to use the most secure method of communication permitted by the particular device.
- The TOE will be configured so as to require the use of HTTPS to access its web-based management GUI.
- 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.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- 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.
- Network devices to be monitored by the TOE are configured to respond to ping or open TCP port requests.
- 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.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.1).
2. This evaluation only covers the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The TOE relies on its operational environment as follows:
    a. 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.

    b. 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.

    c. The supporting database server in the operational environment is relied on to provide secure storage of TSF data, including generated audit records.

    d. 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.

    e. The underlying operating system is relied on to provide a reliable time stamp for use by the TOE.

    f. 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.

g. 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.

h. 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.

i. 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.

j. Network devices must respond to ICMP echo request packets (“ping” packets) or TCP open port requests in order to be discovered by the TOE.

k. 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.

l. The TOE can optionally be configured to use an LDAP or Active Directory server in its operational environment to support authentication of Authorized Users.

m. The TOE relies on the presence of a trustworthy Domain Name System (DNS) server in its operational environment to support hostname resolution.

n. 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.

4. The following product capabilities are restricted from use in the evaluated configuration:

    a. 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:

        i. Initial installation and configuration of the TOE prior to the commencement of live operation, including:

            1. Configuring FIPS 140-2 mode.

            2. Configuring device roles.

            3. Configuring failover.

        ii. Performing database maintenance, including backup and restore.

    b. Use of the Mobile interface to access the TOE.

    c. Use of the web GUI ‘Guest’ account, which is required to be deleted during installation in the evaluated configuration.

    d. Use of the dashboard application, which per guidance authorized administrators are instructed to not use.

5. The following product capabilities were not evaluated and are therefore not included within the scope of the evaluation:

    a. The efficacy of task scripts in performing operations on devices.

    b. The efficacy of Active Script and SSH performance monitors.

c. The efficacy of actions in correcting problems detected on network devices.

d. The efficacy of send/expect language in the monitors.

e. WhatsUp Gold WhatsConnected.

f. WhatsUp Log Management.

g. WhatsUp Gold VoIP Monitor.

h. AlertFox End-User Monitor.

i. WhatsUp Gold Flow Publisher.

j. IP Address Manager.

k. IP v6.

l. Use of ELM (Event Log Management) interfaces to access ELM database functions.

m. Use of AlertFox for web server monitoring and reporting

n. Text-to-speech actions.

o. All notification actions except SMS and email.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and design documentation.

5.1 TOE Architecture

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[1], 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[2]. 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.

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

[1] As noted in Section 4.1, the efficacy of these actions has not been subject to evaluation.

[2] Note that devices on the network being monitored by the TOE are not considered “users” of the TOE.

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 only the following plug-ins 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**. This plug-in 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**. This plug-in 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.

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.

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.

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.

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. 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.

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.

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.

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**. 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.

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.

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.

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.

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 or separately as its own system. 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.

6 Evaluation Evidence

This section provides a list of the evaluation evidence issued by the developer (and sponsor). Documents that are publicly available to customers via the Ipswitch support web site are indicated with *; documents that are not publicly available are indicated with †.

6.1 Guidance documentation

The publicly available guidance documentation examined during the course of the evaluation is as follows:

- *WhatsUp Gold Premium Version 16.1 Common Criteria Supplemental User Guide, Version 2.1, January 14, 2014*.*

- *WhatsUp Gold Release Notes v16.1, March 12, 2013*.*

- *WhatsUp Gold Getting Started Guide v16.1, March 8, 2013*.*
- *Installing and Configuring WhatsUp Gold v16.1, March 11, 2013*.*
- *Using Additional Pollers with WhatsUp Gold v16, March 11, 2013*.*
- *WhatsUp Gold Online Help v16.1, April 2nd, 2013*.*
- *WhatsUp Gold v16.1 Database Migrations and Management Guide, March 9, 2013*.*
- *APM for WhatsUp Gold v16.1 User Guide, February 28, 2013*.*
- *WhatsUp Gold v16.1 Wireless User Guide, February 19, 2013*.*
- *Flow Monitor for WhatsUp Gold v16.1 User Guide, February 19, 2013*.*
- *WhatsVirtual for WhatsUp Gold v16.1 User Guide, February 15, 2013*.*
- *Failover Manager for WhatsUp Gold v16.1 Quick Start Guide, March 11, 2013*.*
- *WhatsUp Gold Failover Manager for WhatsUp Gold v16.1 Deployment and User Guide, March 12, 2013*.*

6.2 Design documentation

- *WhatsUp Gold Premium Version 16.1 Security Architecture ADV_ARC.1, v1.6, December 18, 2013†.*
- *WhatsUp Gold Premium Version 16.1 Functional Specification ADV_FSP.2, v2.0, December 18, 2013†.*
- *WhatsUp Gold Premium Version 16.1 TOE Design Specification Basic Design ADV_TDS.1, v1.8, December 19, 2013†.*

6.3 Lifecycle documentation

- *WhatsUp Gold Premium v16.1 Lifecycle Support Delivery Procedures ALC_DEL.1, Version 1.3, December 18, 2013†.*
- *WhatsUp Gold Premium v16.1 Lifecycle Support CM Capabilities ALC_CMC.2, Version 1.3, December 18, 2013†.*
- *WhatsUp Gold Premium v16.1 Lifecycle Support Configuration List ALC_CMS.2, Version 1.6, January 17, 2014†.*
- *WhatsUp Gold Premium v16.1 Lifecycle Support Basic Flaw Remediation ALC_FLR.1, Version 1.2, October 15, 2013†.*

6.4 Test documentation

- *WhatsUp Gold Premium Version 16.1 Functional Tests ATE_FUN.1, v1.8, November 17 2013†.*
- *WUGv16.1_CommonCriteria_FunctionalTestCases Version 0.8, 11/15/2013 (.xls spreadsheet)†.*
- *WUGv16.1 Reference Document, v0.1, 3/21/2013†.*
- *WUGv16.1 Test Cases, v0.7, 11/13/2013†.*

6.5 Security Target

- *WhatsUp Gold Premium Version 16.1.99 Security Target, Version 1.0, January 16, 2014.*

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the WhatsUp Gold Premium 16.1 software product.

Evaluation team testing was conducted at the vendor's development site December 9-12, 2013.

7.1 Developer Testing

The vendor's test philosophy involves the use of manual test procedures that are based primarily on testing the claimed security functions of the TOE as represented by the SFRs specified in the ST. Essentially, Ipswitch developed a set of test cases that correspond to security functions claimed in the ST, ensuring that all security functions presented at the external interfaces and all TSFI are tested at a level appropriate for EAL2.

Test cases are performed using the Web interface and some third party testing tools. The Web interface is fully tested such that the test cases demonstrate that it fully addresses the admin-related SFRs. The tests consist of both positive and negative testing.

The Ipswitch Test documentation consists of a Test Plan (the ATE_FUN.1 document), a Coverage Analysis document (test case mapping excel spreadsheet), a CC Reference document (containing instructions for various operations needed in the test cases) and a set of Test Case documents (called Test Steps) which include both expected and actual test results. While there is no explicit indication of "Pass" or "Fail", the test case expected and actual results clearly indicate that all test cases are passing.

The Test Plan document describes the overall approach of testing and a description of how the Test Cases are presented. It also includes test configuration information such as test setup, test bed and test tools for the tests. Each test case includes an Introduction, Reference, Product Details, Test Case Description, Test Case Scope, Setup Information, Test Steps, Expected and Actual Results.

The Test Cases are mapped to individual SFRs. The Test Coverage Analysis document provides the definitive mapping of test cases to individual TSFI. The security relevant claims in the TSS were largely covered in vendor testing. Those areas that were determined to be untested were included in the evaluation team testing.

The evaluation team found that the test documentation maps the test cases to the TOE security behaviors identified in the functional specification and TOE design and to the TOE security functional requirements. The evaluation team confirmed the mapping and found that the correspondence between the test documentation and the design documentation is accurate.

7.2 Evaluation Team Independent Testing

The evaluation team exercised the developer and independent tests against the evaluated configuration of the TOE.

The vendor has run all tests across the following two platforms: Windows Server 2003 and Windows Server 2008. The actual results collected are shown for only one platform when the results are exactly the same on all three platforms. These two platforms were chosen because they are based on different versions of NT. Windows 7 is based on NT6.1, which is the same as Server 2008. This also covers both versions of IIS (6 and 7). Microsoft SQL Server 2008 Enterprise, IE 9.x, Firefox 25.0.x and Chrome 23.x browsers were also used in testing.

The evaluation team ran a sample of the vendor test suites across the two platforms. The chosen sample was determined based on the following factors:

- The test subset covers all of the TSFI (WUG application interface, WUG UI interface, Remote Poller interfaces, Device and Application Facing Network interfaces).
- The test subset covers all security functions claimed in the ST with particular attention to the significant security functions for this technology type which are User Data Protection and Network Monitoring.

The following hardware was used to create the test configurations:

- Computer/Workstation running Microsoft Windows 7 to access the Hyper-V host and virtual machines on which the TOE is installed.
- Cisco Switch for Netflow source generation.
- Extreme Networks Switch for sFlow source generation.
- Cisco Wireless LAN controller managing 3 cisco wireless access points.
- Aruba Wireless LAN controller managing 1 wireless access point.
- HP Network Printer.
- UPS – APC Uninterruptable Power Supply.
- Ipswitch Email Server.
- VMware vCenter hosting 4 Vmware hosts.

The following software (including tools used in the vendor tests) was installed on the machines used for the tests:

- WhatsUp Gold Premium with Plug-Ins Version 16.1.99 Build #2376.
- Hyper-V host software.
- Windows 7 Ultimate SP1 (x64).
- Windows 2008 R2 Enterprise SP1.
- Windows Server 2003 R2.
- Active Directory.
- Microsoft SQL Server 2008 Enterprise.
- Linux Ubuntu Server 11.10.
- VMware vCenter.
- Internet Explorer 9.
- Internet Explorer 10.

- Chrome 23.
- Firefox 25.0.
- Wireshark v1.8.6.
- Syslog Generator v1.0.
- TrapGen v2.8.
- Flowalayzer v1.0.0.
- AccessPort v1.37.

The evaluation team performed the following additional functional tests:

- **Auditable Events**—The evaluation team reviewed and collected audit logs for all relevant tests performed during the onsite testing effort. The team also tested that 'create LDAP credential' is audited.
- **Consistent Time—**The evaluation team verified that the TOE timestamp recorded in the audit logs is consistent with the system time in the underlying operating environment.
- **User Rights and Restrictions**—The evaluation team confirmed a number of claims made in the ST regarding user rights and restrictions that were not covered by vendor tests.
- **User Rights and Operations**—The evaluation team confirmed a number of claims made in the ST regarding user rights and operations that were not covered by vendor tests.
- **Group Access Rights—**The evaluation team verified that a user must first have user access rights to a device or group before group access rights are considered and that group access rights are passed from parent group to subgroup.
- **Secure Data Storage—**The evaluation team that the user and device authentication credentials are encrypted in the database.
- **SSHv2 encryption using 3DES—**The evaluation team confirmed the TOE will generate 3DES keys for use with SSHv2 encrypted communication.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE. While there were a few older vulnerabilities that came up in the search, none of them were found to be related to the TOE version and/or they were related to Ipswitch products that are not part of the TOE.

In addition to the open source search, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities. The evaluation team performed the following vulnerability tests:

- **Port and Protocol Scan—**The evaluation team performed a port and protocol scan and confirmed that only necessary ports and services are opened by the TOE during installation.
- **Underlying File Permissions—**The evaluation team identified the TOE components and data stores and verified that appropriate permissions are assigned in the environment.
- **User Input Validation—**The evaluation team verified that attempts to inject SQL commands at the login prompt and to enter invalid data into various fields in the GUI were unsuccessful and resulted in appropriate error messages being generated by the TOE in each case.
- **Log File Checking—**The evaluation team verified that no sensitive data such as unencrypted passwords were found in the log files.
- **Revoked User—**The evaluation team verified that a password change or modification to a user account will take effect at the next user login.
- **Cookie Manipulation—**The evaluation team verified that the GUI interfaces are not vulnerable to session spoofing via cookie manipulation.

8 Evaluated Configuration

The evaluated version of the TOE is identified as the WhatsUp Gold Premium with Plug-Ins Version 16.1.99. The TOE includes only the following plug-ins 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**. This plug-in 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**. This plug-in 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.

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.

TOE Components

This section identifies the components comprising the TOE and the requirements the TOE has for hardware and software in its operational environment. 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 5.1 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.

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.

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 2.

Table 2. Minimum Recommended Hardware Capabilities for WhatsUp Gold

	100 Devices / 500 Monitors minimum recommended	2,500 Devices / 12,500 Monitors minimum recommended	20,000 Devices / 100,000 Monitors minimum recommended

	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

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

[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 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.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an “EAL2 augmented with ALC_FLR.1” certificate rating be issued for WhatsUp Gold Premium Version 16.1.99.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3. TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1:	Basic design
AGD_OPE.1:	Operational user guidance
AGD_PRE.1:	Preparative procedures
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_COV.1:	Evidence of coverage
ATE_FUN.1:	Functional testing
ATE_IND.2:	Independent testing – sample
AVA_VAN.2:	Vulnerability analysis

10 Validator Comments/Recommendations

1. The Letter of Intent (LOI) provided for this evaluation included the WhatsUp Event Log Manager Suite v9, however, this product is being addressed in a separate evaluation.
2. The TOE will not discover all unknown devices on the network, only those that respond in an expected way. Some devices might not have been prepared to respond to the discovery protocols.

11 Annexes

Not applicable.

12 Security Target

The ST for this product’s evaluation is *WhatsUp Gold Premium Version 16.1.99 Security Target, Version 1.0, January 16, 2014.*

13 Acronyms and Abbreviations

API	Applications Programming Interface
APM	Application Performance Monitoring
ASA	Adaptive Security Appliances
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	CCTLCommon Criteria Testing Laboratory
CEM	Common Criteria and Common Methodology for IT Security Evaluation
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
DNS	Domain Name System
ELM	Event Log Management
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ID	Identification
IP	Internet Protocol
IPFIX	IP Flow Information Export
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOI	Letter of Intent
MD	Maryland
MIB	Management Information Base
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NT	New Technology
OS	Operating System
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SP	Service Pack
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TSF Interface
UPS	Uninterruptable Power Supply
U.S.	United States

VoIP	Voice Over Internet Protocol
VR	Validation Report
WAN	Wide Area Network
WCF	Windows Communication Foundation
WMI	Windows Management Instrumentation
WUG	WhatsUp Gold

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009,

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, July 2009.

[4] Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 3, July 2009.

[5] WhatsUp Gold Premium Version 16.1.99 Security Target, Version 1.0, January 16, 2014.