POSITIVE TECHNOLOGIES

MAXPATROL
VULNERABILITY AND COMPLIANCE MANAGEMENT SYSTEM

Common Criteria Certification

Security Target

Author:	Dmitry Kuznetsov, Positive Technologies TÜV Informationstechnik GmbH
Category:	CC Certification

Version:	1.5
Date:	2014-09-29
File Name:	PT_ST_1.5.docx

Abstract

This document is the ST (Security Target) of the MaxPatrol Console and parts of the MaxPatrol Server Common Criteria Certification. Both components belong to the MaxPatrol Compliance and Vulnerability Management System.

Keywords

CC, ST, Common Criteria, Security Target

Prepared for

Positive Technologies
Schelkovskoe shosse 23A
107241 Moscow
Russian Federation

Phone: +7 (495) 744 - 0144

http://www.ptsecurity.com

Prepared by

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstraße 20
45141 Essen, Germany

Phone: +49 (201) 8999 - 9

https://www.tuvit.de

Table of Contents

List of Tables

List of Figures

1 ST Introduction

This chapter presents ST and TOE identification information, summarizes the ST in narrative form and provides information for a potential user to determine whether MaxPatrol Compliance and Vulnerability Management System (CC) is of interest. A ST contains the security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. A ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the operational environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply (chapter 3).

b) A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 6).

c) The security functionality provided by the TOE that meets the set of requirements (chapter 7).

1.1 Security Target and TOE references

Table 1.1 – ST Identification

Title:	MaxPatrol Compliance and Vulnerability Management System Common Criteria Certification Security Target
Short Title:	MaxPatrol ST
Version:	1.5
Date:	2014-09-29
Author:	Dmitry Kuznetsov, Positive Technologies TÜV Informationstechnik GmbH
CertID:	BSI-DSZ-CC-0931

Table 1.2 – TOE Identification

TOE Identification:	MaxPatrol Compliance and Vulnerability Management System (CC) and its related guidance documentation
TOE Short:	MaxPatrol (CC)
TOE Version:	8.25.1.20707
TOE Developer:	Positive Technologies
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 ([CC])
Evaluation Assurance Level:	EAL2
PP Conformance:	none

1.2 TOE overview

The TOE overview summarizes the usage and major security features of the TOE. The TOE overview provides a context for the TOE evaluation by describing the product and defining the specific evaluated configuration.

The TOE is part of a Vulnerability and Compliance Management System that is used to detect potential vulnerabilities within the scanned system or networks. Especially the TOE consists of parts of the MaxPatrol Server and the MaxPatrol Console.

The MaxPatrol Server is the primary part of the Compliance and Vulnerability Management System. It includes a scanning core that is used to scale systems and networks, a report service to create reports, based on the scanned results and a control system to coordinate the different processes. Further, the MaxPatrol Server comprises a knowledge base containing information about security tests and vulnerabilities as well as configuration checklists used to check the compliance of a scanned device to predefined standards. Another part of the MaxPatrol Server is an update service that is used to keep the knowledge base up to date and to update the binaries of the MaxPatrol Server and the MaxPatrol Console.[1] Please note that the knowledge base and the update service are not part of the TOE.

To communicate with the MaxPatrol Server users have to employ the services of MaxPatrol Console, which is also part of the TOE.

In particular the following components comprise the TOE:

- Scanning core, as part of the MaxPatrol Server,
- Report service, as part of the MaxPatrol Server,
- Control system, as part of the MaxPatrol Server, and
- MaxPatrol Console.

The security functionalities of the TOE comprise:

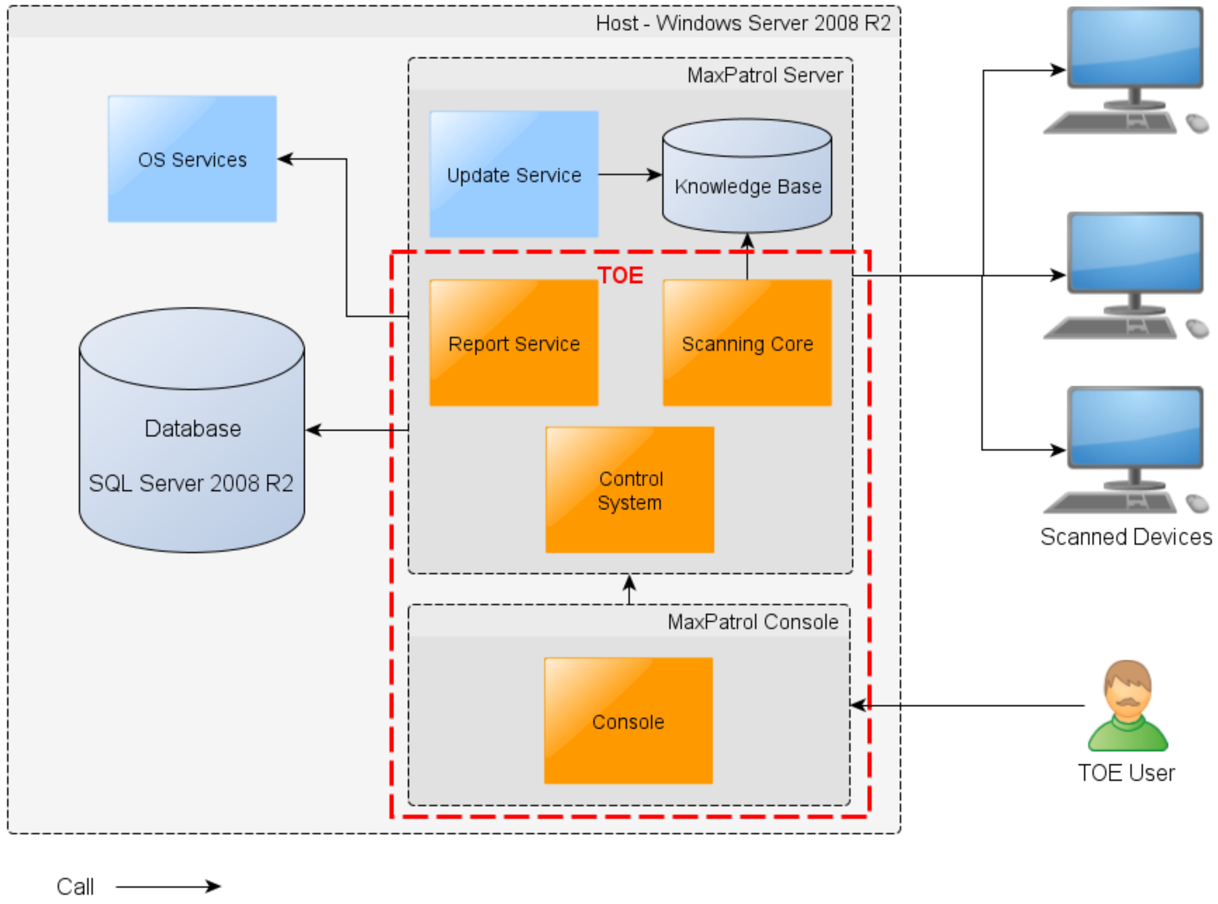
- Security Audit,
- Identification and Authentication,
- Security Management,
- Access Control,
- Scanning and Reporting.

A summary of the TOE security functionality can be found in chapter 1.3.3. Further, a more detailed description is provided within the TOE Summary Specification in chapter 7.

All TOE components as well as the intended operational environment of the TOE are illustrated in Figure 1.1:

[1] According to the guidance documentation the TOE users are not allowed to use the update service to update the binaries of the certified version.

Figure 1.1 – TOE Boundary



1.2.1 Brief description of the TOE components

The TOE consists of a number of components that work together to collect, store and analyze data from a network and report the results to authorized TOE users as well as to implement the security functionality Access Control, Identification and Authentication and Security Audit.

The TOE is part of the MaxPatrol Compliance and Vulnerability Management System and consists of the following components:

- Parts of the MaxPatrol Server, namely the Control System, the Report Service and the Scanning Core.
- MaxPatrol Console to communicate with the MP Server.

The main part of the TOE is the scanning core that implements the scanning functionality. This component performs collects data concerning the used network services and installed software from the attached external devices. Further, it analyzes this data using the information stored in the knowledge base to identify potential vulnerabilities.The reporting service generates reports based on the scanning results. Those reports as well as the scanning results are stored within an external database.

Further, the control system manages the processes within the TOE and is connected to MaxPatrol Console. The MaxPatrol Console is a graphical user interface that is employed by TOE users for configuration and management purposes.

1.2.2 Brief description of the operational environment of the TOE

An overview of the TOE and the immediate operational environment is provided in Figure 1.1. As can be seen within the figure all parts of the TOE are installed on one host. The TOE is a software only product and needs the resources, e.g. reliable timestamps, of an operating system. In general several platforms can be used but for the certified version only Windows Server 2008 R2 is used.

In addition Figure 1.1 shows that the TOE consists of the MP Console and parts of the MP Server as listed in chapter 1.2.1. Other parts of the MP Server are not part of the TOE. Those parts comprise the Update Service and the Knowledge Base. The Knowledge Base is a data base that contains security and technical standards used within the compliance mode and information used by the scanning core to access and scan the devices as well as detect potential vulnerabilities of the scanned devices. In general, the Update Service is used to update the contents of the knowledge base or the software of the MP Server and MP Console. Within the certified version the TOE users are advised by the guidance documentation to use the update service only to update the content of the knowledge base but not the binaries of the MP Server or the MP Console.

Despite the fact that parts of the MP Server are not part of the TOE, the complete installation of the MP Server is required for an operational state of the TOE. Therefore, the MP Server 8.25.1.20707 must be installed on the host.

Furthermore a database is needed to store the scanning results and the reports. The database is not part of the TOE but has to be installed on the same host computer. In general the TOE can interact with several databases but within the evaluation and certification process only Microsoft SQL Server 2008 R2 will be considered.

No requirements are imposed on the scanned devices. An overview of programs that are considered by the TOE to detect potential vulnerabilities can be found in chapter 1.3.1.

For more details on the required operational environment please refer to chapter 1.3.2.

1.3 TOE description

This chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration. The main purpose of this chapter is to bind the TOE in physical and logical terms. The chapter starts with a description of the product type before it introduces the physical scope, the architecture and the logical scope of the TOE.

1.3.1 Product Type

The software application MaxPatrol Compliance and Vulnerability Management System is designed to automate and centralize the processes of vulnerability detection and analyzing the security state of the scanned devices, whereby a scanned device can represent a system or a network. Especially the system is able to perform the following applications:

- inventory of hardware and software of the scanned devices,
- identification of vulnerabilities, including the vulnerabilities caused by configuration errors,
- evaluation of the compliance of the configuration of the scanned device to predefined requirements and standards,
- generation of reports on the current security level of the scanned device and changes to the previous state of the scanned system or network,
- detection of security relevant events that are related to unauthorized modification of software and hardware of the scanned devices, and the prevention of related security incidents,
- assessment of actions that are applied to correct security vulnerabilities.

MaxPatrol Compliance and Vulnerability Management System provides a set of general tests used to find vulnerabilities of web-based applications and performs security analysis for the following software:

- Operating systems: Microsoft Windows 2000/2003/XP/Vista/2008/7, Solaris 8/9/10, RedHat Enterprise Linux, FreeBSD, HP-UX 11.0, AIX and Mac OS;
- Groupware: Microsoft Exchange Server 2000-2010 and Lotus Domino;
- Database Management Systems: Microsoft SQL Server 2000-2008 and Oracle Database Server 9-11;
- Information system based on SAP NetWeaver 6.4/7.0;
- Network Applications: Cisco, Huawei, Nortel, Alcatel;
- Firewalls: Cisco, CheckPoint and Juniper;
- Microsoft Office 2003, 2007;
- Anti-Virus Software: Kaspersky, Symantec, Dr.WEB, Eset, Trend Micro.

MaxPatrol Compliance and Vulnerability Management System differentiates between three scanning modes:

- PenTest – Network Scanning
  Within the PenTest mode the scanning of the network is provided using a minimum set of privileges on the scanned device. The purpose of this mode is to obtain the security assessment by an external attacker. Therefore, the MaxPatrol System has to identify potential vulnerabilities regarding the used web applications, network services and operating system. Furthermore the strength of password is checked by performing brute force attacks.
- Audit – System Scanning
  The aim of the Audit mode is to get an overview of the security level of the operation system and the installed software of the external devices from the perspective of an local user. Therefore the MaxPatrol System maintains account information to get access to the external devices.
- Compliance – Compliance Control

Within the Compliance mode the MaxPatrol System evaluates the compliance of the scanned devices to predefined standards that are maintained within the knowledge base.

Based on the scanning results MaxPatrol Compliance and Vulnerability Management System generates reports and provides them to authorized entities. In addition the MaxPatrol System is able to log user actions and events as well as to provide an access control and an identification and authentication mechanism.

The minimal deployment configuration of the MaxPatrol Compliance and Vulnerability Management System consists of a MP Server and a MP Console. Basically the MP Server consists of the following components:

- Knowledge Base – contains a configuration checklist that is needed within the Compliance Mode and information used to access and scan the devices as well as detect potential vulnerabilities,
- Scanning Core – implements the scanning process,
- Update Service – updates content of the knowledge database as well as the binaries of the MP Server and the MP Console,[2]
- Report Service – generates reports based on the scanning results,
- Control System – manages the different processes of the MP Server.

MaxPatrol Console is a graphical user interface that is used by administrators to communicate with the MP Server.

In general additional MP Servers, MP Scanners, which represent the scanning core of the MP Server and a MP Consolidation Server can be attached to the system, but within the certification process only the minimal deployment configuration is considered, whereby it is assumed that the MP Server and the MP Console are installed on the same machine.

The TOE itself is part of the MaxPatrol Compliance and Vulnerability Management System and consists of parts of the MaxPatrol Server and the MaxPatrol Console (cf. chapter 1.3.2). Please note that the Update Service and the Knowledge Base are not part of the TOE (cf. chapter 1.2.1).

1.3.2 Physical scope

Figure 1.1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the operational environment of the TOE. The TOE is a software only product and the TOE components are specified in Table 1.3 below:

Table 1.3 – TOE identification and boundary

TOE Component	Description
Control System	The Control System is part of the MaxPatrol Server. This component

[2] For the certified version the users are advised within the guidance documentation to use the update service only to update the content of the knowledge base and not the TOE binaries.

	communicates with the MaxPatrol Console and manages the processes within the TOE.
Report Service	The Report Service is part of the MaxPatrol Server. This component generates reports based on the scanning results. The content and structure of the reports depends on templates configured by authorized TOE users.
Scanning Core	The Scanning Core is part of the MaxPatrol Server. This component implements the scanning process for network checks and brute force attacks (PenTest mode), system checks (Audit mode) and compliance control (Compliance mode).
Console	Console represents the MaxPatrol Console which is a graphical user interface. Its services are employed by TOE users to communicate with the TOE and to configure the MP Server.

In addition the following guidance documents are part of the TOE:

- MaxPatrol Compliance and Vulnerability Management System – Administrator Guide,
- MaxPatrol – Installation Guide,
- MaxPatrol – Quick Start Guide,
- MaxPatrol Help File (MaxPatrol_en),
- MaxPatrol Compliance and Vulnerability Management System – Guidance Addendum.

The TOE accompanied by its guidance documentation and an individual license file is provided to customers as a downloadable archive or via mail on a DVD. Further, a notification letter that contains SHA-512 checksums for every file of the downloadable archive or the DVD is sent to the respective customer separately via e-mail, fax or express delivery.

Figure 1.1 shows the immediate operational environment of the TOE:

- **Microsoft Windows Server 2008 R2** is the operating system which hosts the TOE. The TOE uses several resources of the OS. These resources comprise general functionality as well as specific functionality of the OS, which is necessary for the security functionality of the TOE (e.g. reliable timestamps).
- **SQL Server 2008 R2** is the database which is used by the TOE to store the scanning results and reports as well as user authentication data and account data. The database has to be installed on the same machine as the TOE itself.
- Parts of **MaxPatrol Server**, which are not part of the TOE, are nevertheless used by the TOE to perform the security functionality correctly. Especially the knowledge base that contains information about potential vulnerabilities and standards used within the Compliance Mode is utilized by the TOE to collect and analysis the data from the

attached devices. The update service of the MP Server is used to update the content of the knowledge base.[3]

Table 1.4 below specifies the minimum hardware and software requirements for the TOE.

Table 1.4: TOE minimum requirements

Aspect	Requirements
CPU	Intel® Pentium® 4 processor 2,2 GHz
RAM	4 GB
HDD	50 GB
OS	Microsoft Windows 2008 R2 Enterprise (x64) (including the .NET framework 4.0)
DB	Microsoft SQL Server 2008 R2
Other Software	MP Server 8.25.1.20707[4]

1.3.3 Logical scope

The logical boundary of the TOE is divided into the following security classes which are described in detail within the chapters 6 and 7. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Functionality:

1.3.3.1 Security Audit

The TOE records the performed management actions on the TOE as well as each identification and authentication attempt. Authenticated users are allowed to view the audit records to ensure that the users have the possibility to detect potential attacks or misconfiguration of TOE security features. A further purpose of the audit functionality is to hold users accountable for any actions they perform regarding the configuration of TOE Security Functions.

1.3.3.2 Identification and Authentication

The TOE provides a mechanism for identification and authentication of users who communicates with the TOE. In addition the TOE offers the possibility to use an identification and authentication mechanism of the underlying operating system.[5]

[3] In general, the Update Service can also be used to update the software of the MP Server and MP Console. For the certified version the users are advised within the guidance documentation to use the update service only to update the content of the knowledge base and not the TOE binaries.

[4] Not all parts of the MP Server are part of the TOE. Nevertheless the complete MP Server must be installed on the host.

[5] Note that the TOE as well as the underlying operating system provides a mechanism for identification and authentication. For more details please refer to Chapter 7.5.

1.3.3.3 Security Management

The TOE provides a set of functionalities to manage the security functions, configuration, and other features of the TOE components by authorized user roles.

1.3.3.4 Security Access

This function of the TOE controls the access of user groups to data protected by the TOE, whereby it uses an access control policy based on roles. It further controls that only authorized user roles can manage the TOE. Especially the access control policy ensures that only administrators are able to crate user accounts and user groups and set privileges to them.

1.3.3.5 Scanning and Reporting

The Scanning and Reporting function performs the collection of system data of the scanned devices, analysis of the collected data, and generation of reports based on the analysis. For the scanning and analysis functionality the TOE differentiates between three different modes (cf. chapter 1.3.1):

- PenTest – Network scanning,
- Audit – System scanning, and
- Compliance – Compliance control.

1.4 Conventions

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>underlined text within brackets</u>].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using “EXT_” at the beginning of the short name.
- Iterations are identified by appending a number in parentheses following the component title. For example, FAU_GEN.1 (1) Audit Data Generation would be the first iteration and FAU_GEN.1 (2) Audit Data Generation would be the second iteration.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. This chapter contains the following sections:

- CC conformance claims
- PP claim
- Package claim
- Conformance rationale

2.1 CC conformance claims

This Security Target claims to be conformant to the Common Criteria 3.1:

- Part 2 extended to [CC]

  In order to provide a complete description of the functional requirements addressed by the TOE, functional components of part 2 of the Common Criteria framework were used. But also additions to the Common Criteria part 2 were defined, to fulfill the requirement of a complete and consistent TOE description.

- Part 3 conformant to [CC]

  For the description of the requirements due to the trustworthiness of the TOE, only security assurance requirements of CC part 3 were used.

2.2 PP claim

This ST does not claim conformance to any PP.

2.3 Package claim

This Security Target claims to be conformant to the Security Assurance Requirements package EAL 2.

2.4 Conformance rationale

This ST does not claim conformance to any PP.

3 Security Problem Definition

This section describes the security aspects of the operational environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It describes

- the assets that have to be protected by the TOE,
- threats against those assets,
- organizational security policies that TOE shall comply with, and
- assumptions about the operational environment of the TOE.

3.1 Assets

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

Table 3.1 – Assets

Assets	Description
Account	Identification and Authentication data that is used by the TOE to get access to the scanned devices.
Active scans	Active scanning process and the corresponding scanning results.
Audit records	Log data of the TOE. It contains information on security relevant events as well as on security relevant operations performed by TOE users.
Compliances	Data to check the compliance of the scanned devices within the Compliance mode.
Deliveries	Configuration data that defines the parameters for the delivery of reports.
Dictionaries	Data, e.g. possible usernames and passwords, vulnerability groups, which is used by the TOE during the scanning process.
Groups	Groups of vulnerabilities or software which are used within the scanning processed and referenced by dictionaries.
Identification rules	Rules used to identify a host that shall be accessed. Identification rules are referenced by tasks.
Overrides for variables	Compliance overrides used within the Compliance mode, they are referenced by Profiles.
Profiles	Configuration data that defines the parameters and references the account used for the scanning process.
Reports	Scanning results of one or more tasks in a user-friendly structured and filtered format. Therefore a chosen report template is applied to a chosen scan of a specified task.
Report Template	Configuration data that defines the parameters which are used to generate a report.
Scan / Scanning results	Results of the scanning process performed by the TOE on the scanned devices.
Schedule	Scripts that allows authorized users to automate and plan the systems activity.
Tasks	Configuration data that defines the settings for a scanning process and references the profile and identification rules that should be used.

Assets	Description
User authentication data	User authentication data that is maintained by the TOE.
TSF data	Data for the operation of the TOE upon which the enforcement of the SFR relies. It contains • system configuration parameters, • user authentication data, • audit records, • account data, • active scans, • compliances, • dictionaries, • identification rules, • scanning and report configuration parameters (Deliveries, Profiles Report Templates, Schedules, and asks).
User data	Data for the TOE users that does not affect the operation of the TSF. It contains • scanning results and reports, • data managed by the scanned external devices.

3.2 Subjects

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

Table 3.2 – Subjects

Subject	Description
Attacker	An entity who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets protected by the TOE. They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
Administrator	An authenticated user who has unrestricted access to all TOE functionalities. Administrators are responsible for the management of all TOE process and have to ensure that the TOE operates in a secure way. Especially only Administrators are allowed to create, remove and change users, user groups and object owners, but they are not able to view passwords of TOE users or of the account that are used for the scanning process.
IT-Administrator	An authenticated user who is responsible for creating and changing the accounts that are necessary to access the scanned devices.
Manager	An authenticated user who maintains the reports of the scanning results. The Manager is allowed to view the scanning results as well as to create reports and specify the delivery of the reports.
Operator	An authenticated user who is responsible for the scanning processes and is able to use the predefined tasks.

Subject	Description
Authenticated User	A user who has been identified and authenticated by the TOE or an identification & authentication mechanism provided by the underlying operating system and accepted by the TOE (Administrators, IT Administrators, Manager and Operator).
Unauthorized User	An authenticated user who is not authorized to perform a certain operation.

3.3 Threats

The table below identifies the threats to the assets against which protection is required by the TOE:

Table 3.3 – Threats

Threat	Description
T.CONFIG	The TOE may be configured in such a way that attackers or unauthorized users may gain unauthorized access to user or TSF data.
T.EXPLOIT	An attacker may attempt to gain unauthorized access to the data managed by the scanned external devices, by exploiting vulnerabilities on a scanned external device.
T.MASQUERADE	An attacker may masquerade as an authorized user in order to gain unauthorized access to TSF data or user data.
T.UNAUTH	An attacker or a TOE user may gain unauthorized access to the TOE and disclose TSF data or user data and/or modify the behavior of the TOE in an unsecure way.
T.UNDETECTED	The security relevant actions of users may go undetected making the TSF data vulnerable to attack. An attacker could exploit these circumstances to get unauthorized access or to modify the behavior of the TSF.

3.4 Organizational security policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE.

There is no organizational security policy defined for the TOE or the operational environment.

3.5 Assumptions

This section describes the security aspects of the intended operational environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

The assumptions about the TOE’s security environment are defined in Table 3.4 below.

Table 3.4 – Assumptions

Assumption	Description
A.AUTHEN	The underlying OS provides an identification and authentication mechanism for TOE users.[6]
A.MANAGE	The users who manage the TOE as well as all administrators of the host, where the TOE is installed on, are non-hostile, appropriately trained, and follow all guidance documentation.
A.PROTECT	The TOE is located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.STORAGE	The operational environment provides the availability to store data within an external database. The database is located at the same machine as the TOE itself and it is ensured that only authorized users are allowed to access the TSF data stored within this database.
A.OS	The underlying OS provides the TOE with the necessary reliable timestamps and services of file protection as well as cryptographic support.

[6] The TOE provides the possibility to use two different identification and authentication mechanisms, one performed by the TOE itself, one by the underlying operating system.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see chapter 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE‟s operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security objectives for the TOE

TOE security objectives are defined in Table 4.1, below.

Table 4.1 – Security Objectives for the TOE

Objective	Description
O.ACCESS	The TOE must enforce an access control policy to ensure that only users who are authorized to access the relevant data are able to do so.
O.AUDIT	The TOE must provide the means of recording the performed management actions on the TOE as well as each identification and authentication attempt, so as to assist corresponding users in the detection of potential attacks or misconfiguration of TOE security features as well as hold users accountable for any actions they perform regarding the configuration of TOE Security Functions.
O.AUTH	The TOE must provide a mechanism for identification and authentication of users who communicate with the TOE.
O.MANAGE	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such control.
O.SCAN	The TOE must be able to collect information from external devices, analyze the information and generate reports based on the scanning results.

4.2 Security objectives for the operational environment

The security objectives for the TOE operational environment are based on the secure usage assumptions and defined in Table 4.2 below.

Table 4.2 – Security Objectives for the operational environment

Objective	Description
OE.AUTHEN	The underlying OS must provide an identification and authentication mechanism for TOE users.
OE.MANAGE	TOE users who are responsible for the TOE must be competent, non-hostile, appropriately trained and follow all guidance documentation.

Objective	Description
OE.PROTECT	Those responsible for the TOE must ensure that the physical environment must be suitable for supporting a computing device in a secure setting.
OE.STORAGE	The operational environment must provide the availability to store data within an external DB. The DB must be located at the same machine as the TOE itself.
OE.OS	The underlying OS must provide reliable timestamps and file protection as well as cryptographic support for the TOE.

4.3 Security objectives rationale

Table 4.3 – Security Objectives rationale

Threats and Assumptions vs. Security Objectives	O.ACCESS	O.AUDIT	O.AUTH	O.MANAGE	O.SCAN	OE.AUTHEN	OE.MANAGE	OE.PROTECT	OE.STORAGE	OE.OS
T.CONFIG				X						
T.EXPLOIT					X					
T.MASQUERADE			X							
T.UNAUTH	X		X	X						
T.UNDETECTED		X								
A.AUTHEN						X				
A.MANAGE							X			
A.PROTECT								X		
A.STORAGE									X	
A.OS										X

T.CONFIG is countered by

- O.MANAGE since this TOE security objective ensures that the TOE provides a set of management functions that allow a secure configuration of the TOE. Further this objective ensures that only users with appropriate privileges are able to manage the TOE.

T.EXPLOIT is countered by

- O.SCAN since this TOE security objective ensures that the TOE collects information from the scanned devices, analyzes the data and generates reports based on the scanning results.

T.MASQUERADE is countered by

- O.AUTH since this TOE security objective provides an authentication and identification mechanism.

T.UNAUTH is countered by a combination of

- O.MANAGE since this TOE security objective ensures that only users with appropriate privileges are able to manage the TOE, and
- O.ACCESS since this TOE security objective ensures that an access control policy is applied, which ensures that only users who are authorized to access sensitive data are able to do so.
- O.AUTH since this TOE security objective provides an authentication and identification mechanism.

T.UNDETECTED is countered by a combination of

- O.AUDIT since this TOE security objective ensures that the performed management actions on the TOE as well as each identification and authentication attempt are recorded.

As can be seen above every identified threat is countered by one or more security objectives as defined in Table 4.1.

A.AUTHEN is addressed by

- OE.AUTHEN, since OE.AUTHEN ensures that the underlying OS provides an identification and authentication mechanism for the TOE.

A.MANAGE is addressed by

- OE.MANAGE, since OE.MANAGE ensures that users who manage the TOE are non-hostile, appropriately trained, and follow all guidance documentation.

A.PROTECT is addressed by

- OE.PROTECT, since OE.PROTECT ensures that the TOE operational environment provides protection from external interference or tampering.

A.STORAGE is addressed by

- OE.STORAGE, since OE.STORAGE ensures that the TOE operational environment provides the availability to store data within an external DB that is located at the same machine as the TOE itself.

A.OS is addressed by

- OE.OS, since OE.OS ensures that the underlying OS provides reliable timestamps and file protection to the TOE.

Every assumption is addressed by one objectives for the operational environment. The justification above demonstrates that the defined security objectives for the operational environment uphold all defined assumptions.

There is no OSP defined. Therefore no rational is needed.

5 Extended Components Definition

This chapter defines TOE security functional requirements and assurance requirements which are not part of CC 3.1 part 2 or part 3.

The assurance requirements that have been defined by the Common Criteria v3.1 part 3 are applicable to the extended components.

Because this component is a software component with a well-defined behavior on its external interfaces, the assurance requirements that have been defined in part 3 of Common Criteria are applicable to this functional family.

Through its nature as a software component the assurance classes ADV, AGD, ALC, ATE and AVA are applicable in the evaluation process. It is not required to define a new assurance class or assurance family for a consistent and complete description to cover this SFR. This SFR does not define any behavior that might require an extension of part 3 of the Common Criteria Evaluation Framework.

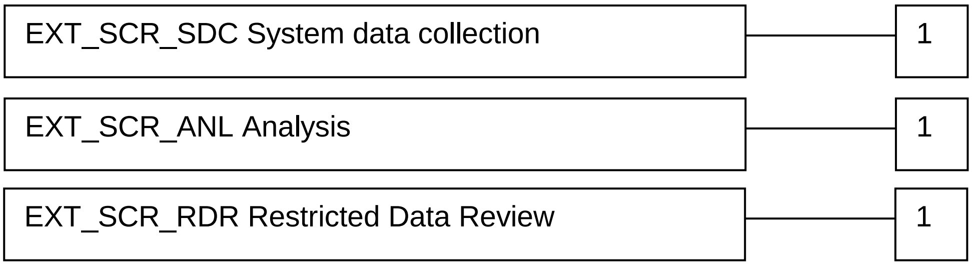
5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE.

5.1.1 Class EXT_SCR: Scanning and Reporting

The Scanning and Reporting functionality involves collecting information from scanned devices, analyzing the data for potential vulnerability and compliance to predefined standards, and providing reports on the findings. The EXT_SCR Scanning and Reporting functionality class was defined because part II of [CC] does not contain any SFR which defines scanning of external devices, analyzing the collected data and creating of summery reports.

Figure 5.1 – EXT_SCR: Scanning and Reporting class decomposition


EXT_SCR_SDC System data collection
1
EXT_SCR_ANL Analysis
1
EXT_SCR_RDR Restricted Data Review
1

5.1.1.1 System data collection (EXT_SCR_SDC)

Family Behavior

This family defines the requirements for collecting data. This family identifies the level of system data collection, enumerates the types of information that shall be collected by the TSF, and identifies the minimum set of SCR-related information that should be provided within various SCR record types.

Component leveling

EXT_SCR_SDC.1 System data collection, defines the level of information, and specifies the list of data that shall be recorded within the scanning results.

Management: EXT_SCR_SDC.1

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

a) Configuration of the scanning process.

Audit: EXT_SCR_SDC.1

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

a) All management actions regarding the configuration of the scanning process.
b) The start and stop of the scanning process.

EXT_SCR_SDC.1 System data collection

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamp

EXT_SCR_SDC.1.1 The TSF shall be able to collect the following information from the scanned device(s): [assignment: *specifically defined information*]

EXT_SCR_SDC.1.2 At a minimum, the TSF shall record the following information: [assignment: *information that shall be recorded*].

5.1.1.2 Analysis (EXT_SCR_ANL)

Family Behaviour

This family defines the analysis the TOE performs on the collected application and change control data. This family also determines which changes are to be prevented, and which are to be monitored and reported.

Component leveling

EXT_SCR_ANL.1 Application and change control analysis, specifies the list of analyses the TOE will perform on the collected application data.

Management: EXT_SCR_ANL.1

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

a) Configuration of the analysis that shall be performed.

Audit: EXT_SCR_ANL.1

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

a) All management actions regarding the configuration of the scanning process.

EXT_SCR_ANL.1 Analysis

Hierarchical to: No other components

Dependencies: EXT_SCR_SDC.1 System data collection

EXT_SCR_ANL.1.1 The TSF shall perform the following analysis function(s) on the collected data: [assignment: *analytical functions*].

5.1.1.3 Restricted data review (EXT_SCR_RDR)

Family Behaviour

This family defines the requirements for system data tools that should be available to authorized users to assist in the review of system data.

Component leveling

EXT_SCR_RDR.1 Restricted data review, the TSF shall provide the System data in an understandable form only to authorized users.

Management: EXT_SCR_RDR.1

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

a) Management of the configuration used to generate reports.

Audit: EXT_SCR_RDR.1

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

a) All management actions regarding the configuration of report generation.
b) All report generation attempts.

EXT_SCR_RDR.1 Restricted Data Review

Hierarchical to: No other components

Dependencies: EXT_SCR_SDC.1 System data collection
EXT_SCR_ANL.1 Analysis
FMT_SMR.1 Security roles

EXT_SCR_RDR.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of data*].
EXT_SCR_RDR.1.2	The TSF shall provide the collected data in a manner suitable for the user to interpret the information.
EXT_SCR_RDR.1.3	The TSF shall prohibit all users read access to the collected data, except those users that have been granted explicit read-access.

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This chapter defines the IT security requirements that shall be satisfied by the TOE or its operational environment:

Common Criteria divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g. configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subchapters.

6.1 Security functional requirements

The specified functional requirements are compliant with Common Criteria v3.1 part 2 and are corresponding with the given functional components.

Table 6.1 – TOE Security Functional Requirements

Name	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_UAU.5	Multiple authentication mechanism
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
EXT_SCR_SDC.1	System data collection
EXT_SCR_RDR.1	Restricted data review
EXT_SCR_ANL.1	Analysis

6.1.1 Class FAU – Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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) [*all identification and authentication attempts (success and failure) as well as all actions that are listed in Table 6.2 except for View and Use operations].*

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, [*none*].

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*all authenticated users*] with the capability to read [*all 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.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.1.2 Class FIA – Identification and authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *User identifier (Login)*
- *Role (Group membership)*
- *Type of login*
- *In addition only for Windows authentication: corresponding domain name*
- *In addition only for MaxPatrol authentication: hashed*[7] *password*].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [

- *MaxPatrol Authentication*
- *Access to Windows Authentication*

] to support user authentication.

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

- *if the flag "Login with current Windows credentials" is set the Windows authentication mechanism is used,*
- *otherwise the MaxPatrol authentication mechanism is used*].

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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.

[7] The hashing is performed by the underlying OS via SHA1.

6.1.3 Class FDP – Access control policy

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Role-based access control policy*] on [

- *Subjects: all authenticated users*
- *objects as listed in the second column of Table 6.2 and*
- *all operations listed in the first column of Table 6.2*].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Role-based access control policy*] to objects based on the following: [

- *The user identity and group membership that is associated with a role,*
- *operations on objects, and*
- *objects*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *If the requested operation on the requested object is permitted to the role that is associated with a group of which the authenticated user is a member (cf. Table 6.2), grant access,*
- *else deny access*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.1.4 Class FMT – Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Role-based access control policy*] to restrict the ability to [*manage*] the security attributes [*of the objects listed in Table 6.2*] to [*the authorized user roles as specified in Table 6.2*].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Role-based access control policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*no one*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete, clear, [*and other operations as defined in column „Operation“ of Table 6.2*]] the [*objects as defined in column „Objects“ of Table 6.2*] to [*the authorized identified roles as defined in column „Authorized Role“ of Table 6.2*].

Table 6.2 – Management Functions

Operation	Objects	Authorized User Roles
Edit, View	Server settings	Administrator
Edit, View	Interserver communications	Administrator
Create, Delete, Edit, View	Users, user groups	Administrator
Create, Delete, Edit, View settings	Tasks	Administrator
Start	Tasks	Administrator, Operator
View results	Tasks	Administrator, Manager
Pause, Cancel, Continue, View	Active Scans	Administrator, Operator
Create, Delete, Edit, Use, View ID[8]	Accounts	Administrator, IT-Administrator
Create, Delete, Edit, Use, View	Dictionaries	Administrator, Manager

[8] No user is able to see the password of the account.

Operation	Objects	Authorized User Roles
Create, Delete, Edit, Use, View	Profiles	Administrator
Create, Delete, Edit, Use, View	Compliances	Administrator
Create, Delete, Edit, Start, Cancel, Pause, Continue, View	Schedules	Administrator
Create, Delete, Edit, View	Report Templates	Administrator, Manager
Generate, View	Reports	Administrator, Manager
Create, Delete, Edit, Use, View	Deliveries	Administrator, Manager
Create, Delete, Edit, Use, View	Overrides for variables	Administrator
View	Scanning results	Administrator, Manager
Create, Delete, Edit, Use, View	Identification rules	Administrator

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions [*see Table 6.2*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*as listed in Table 6.3*].

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

Table 6.3 – TOE Roles

Subject	Description
Administrator	An authenticated user who has unrestricted access to all TOE functionalities. Administrators are responsible for the management of all TOE process and have to ensure that the TOE operates in a secure way. Especially only Administrators are allowed to create, remove and change users, user groups and object owners, but they are not able to view passwords of TOE users or of the account that are used for the scanning process.

Subject	Description
IT-Administrator	An authenticated user who is responsible for creating and changing the accounts that are necessary to access the scanned devices.
Manager	An authenticated user who maintains the reports of the scanning results. The Manager is allowed to view the scanning results as well as to create reports and specify the delivery of the reports.
Operator	An authenticated user who is responsible for the scanning processes and is able to uses the predefined tasks.

6.1.5 Class EXT_SCR – Scanning and Reporting

EXT_SCR_SDC.1 System data collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

EXT_ SCR_SDC.1.1 The TSF shall be able to collect the following information from the scanned device(s): [

- *within the PenTest scanning mode information regarding the*
  - *identified network services that uses TCP or UDP,*
  - *identified vulnerabilities concerning the identified services,*
  - *password strength after performing a brute force attack,*
  - *identified operating system.*
- *Within the Audit scanning mode information regarding the*
  - *Installed software and security updates,*
  - *remaining software vulnerabilities,*
  - *hardware.*
- *Within the Compliance scanning mode information regarding the*
  - *information whether the system is compliant to predefined standards.*
-]

EXT_ SCR_SDC.1.2 At a minimum, the TSF shall collect and record the following information:[

- *within the PenTest mode:*
    - *Date and Time when the scan was performed,*
    - *Identification of the scanned nodes*[9]*,*
    - *open ports, protocols and services that are used within the network,*
    - *identified vulnerabilities and the recommendation how the vulnerability can be removed,*
    - *identified version of the operating system.*
- *within the Audit mode:*
    - *Date and Time when the scan was performed,*
    - *Identification of the scanned nodes*[9]*,*
    - *identified vulnerabilities,*
    - *identified version of the operating system,*
    - *identified hardware and software.*
- *within the Compliance mode:*
    - *Date and Time when the scan was performed,*
    - *Identification of the scanned nod*es[9],
    - *statement whether the scanned system/network is compliant to corresponding standards,*
    - *recommendations how to achieve the compliance.*

]

EXT_SCR_ANL.1 Analysis

Hierarchical to: No other components.

Dependencies: EXT_SCR_SDC.1 System data collection

EXT_SCR_ANL.1.1 The TSF shall perform the following analysis function(s) on the collected data: [

- *comparing collected system data at some point in time with those of another point in time to detect the differences (baseline);*
- *comparing collected system data with a set of standards;*
- *comparing collected system data with a set of exceptions.*]

EXT_SCR_RDR.1 Restricted data review

Hierarchical to: No other components.

Dependencies: EXT_SCR_SDC.1 System data collection
EXT_SCR_ANL.1 Analysis
FMT_SMR.1 Security roles

[9] E.g. IP address, hostname or FQDN.

EXT_SCR_RDR.1.1 The TSF shall provide [*the users associated with the roles administrator and/or manager*] with the capability to read [*all collected information*].

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

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

6.2 Security assurance requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2). They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in Table 6.4.

Table 6.4 – EAL Security Assurance Requirements

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
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security problem definition
ASE_TSS.1	TOE summary specification
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.2	Vulnerability analysis

6.3 Security requirement rationale

6.3.1 Rational for the security functional requirements

Table 6.5 – Fulfillment of Security Objectives

Security Objectives vs. Security Requirements	**O.ACCESS**	**O.AUDIT**	**O.AUTH**	**O.MANAGE**	**O.SCAN**
FAU_GEN.1		X			
FAU_GEN.2		X			
FAU_SAR.1		X			
FAU_SAR.2	X	X			
FIA_ATD.1			X		
FIA_UAU.2	X		X		
FIA_UAU.5			X		
FIA_UID.2	X		X		
FDP_ACC.1	X				
FDP_ACF.1	X				
FMT_MSA.1	X			X	
FMT_MSA.3	X				
FMT_MTD.1	X			X	
FMT_SMF.1				X	
FMT_SMR.1	X			X	
EXT_SCR_ANL.1					X
EXT_SCR_SDC.1					X
EXT_SCR_RDR.1	X				

O.ACCESS

- FAU_SAR.2 – This requirement meets the objective O.ACCESS by ensuring that only authenticated users are allowed to review audit records.
- FDP_ACC.1 – This requirement meets the objective O.ACCESS by ensuring that the access control SFP is enforced by the TOE.
- FDP_ACF.1 – This requirement meets the objective O.ACCESS by ensuring that the rules regarding the access control are applied.
- FIA_UAU.2 – This requirement realizes the objective O.ACCESS since it requires that each user has to be successfully authenticated before any other action.

- FIA_UID.2 – This requirement realizes the objective O.ACCESS since it requires that each user has to be successfully identified before any other action.
- FMT_MSA.1 – This requirement meets the objective O.ACCESS by ensuring that only authorized users are allowed to manage the security attributes.
- FMT_MSA.3 – This requirement meets the objective O.ACCESS by ensuring that no one is allowed to specify alternative initial values to override the default values.
- FMT_MTD.1 – This requirement meets the objective O.ACCESS by ensuring that the management of TSF data is restricted to authorized user roles.
- FMT_SMR.1 – This requirement meets the objective O.ACCESS by ensuring that the TOE associates users with roles to provide access to TSF management functions and assets protected by the TOE.
- EXT_SCR_RDR.1 - This requirement meets the objective O.ACCESS by ensuring that only authorized users are able to read the collected information from the scanned devices.

O.AUDIT

- FAU_GEN.1 – This requirement meets this objective O.AUDIT by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
- FAU_GEN.2 – This requirement meets the objective O.AUDIT by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
- FAU_SAR.1 – This requirement meets the objective O.AUDIT by ensuring that authenticated users are able to review logs.
- FAU_SAR.2 – This requirement meets the objective O.AUDIT by ensuring that only authenticated users are able to read the audit records.

O.AUTH

- FIA_ATD.1 – This requirement meets the objective O.AUTH by defining attributes of the users that are necessary for a secure identification and authentication mechanism.
- FIA_UAU.2 – This requirement realizes the authentication part of the objective O.AUTH since it requires that each user has to be successfully authenticated.
- FIA_UAU.5 – This requirement realized the objective O.AUTH by defining the identification and authentication mechanisms that are accepted by the TOE.
- FIA_UID.2 – This requirement realizes the identification part of the objective O.AUTH since it requires that each user has to be successfully identified.

O.MANAGE

- FMT_MSA.1 – This requirement meets the objective O.MANAGE by ensuring that only authorized users are able to manage the security attributes.
- FMT_MTD.1 – This requirement meets the objective O.MANAGE by ensuring that only authorized users are allowed manage the TSF data.

- FMT_SMF.1 – This requirement meets the objective O.MANAGE by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
- FMT_SMR.1 – This requirement meets the objective O.MANAGE by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.

O.SCAN

- EXT_SCR_ANL.1 – This requirement meets the objective O.ANALYZE by ensuring that the TOE analyzes the collected data.
- EXT_SCR_SDC.1 – This requirement meets the objective O.SCAN by ensuring that the TOE collects information from the scanned devices.

6.3.2 Dependencies of security functional requirements

Table 6.6 – Dependencies of security requirements

Requirement	Dependency	Fulfilled
FAU_GEN.1	FPT_STM.1	FPT_STM.1 is not included because time stamps are provided by the operational environment. An environmental objective states that the TOE will receive reliable timestamps provided by the underlying operating system.
FAU_GEN.2	FIA_UID.1	Yes, by FIA_UID.2 that is hierarchical to FIA_UID.1.
	FAU_GEN.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FIA_ATD.1	No dependencies	n/a
FIA_UAU.2	FIA_UID.1	Yes, by FIA_UID.2
FIA_UAU.5	No dependencies	n/a
FIA_UID.2	No dependencies	n/a
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3	Yes
FMT_MSA.1	FDP_ACC.1	Yes
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	Yes

Requirement	Dependency	Fulfilled
FMT_MTD.1	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	Yes, by FIA_UID.2 that is hierarchical to FIA_UID.1.
EXT_SCR_ANL.1	EXT_SCR_SDC.1	Yes
EXT_SCR_RDR.1	EXT_SCR_SDC.1	Yes
	EXT_SCR_ANL.1	Yes
	FMT_SMR.1	Yes
EXT_SCR_SDC.1	FPT_STM.1	FPT_STM.1 is not included because time stamps are provided by the operational environment. An environmental objective states that the TOE will receive reliable timestamps provided by the underlying operating system.

6.3.3 Rational for the assurance requirements

EAL2 was selected because it is the first time this particular TOE is going to be evaluated. Therefore and in order to keep evaluation efforts reasonable a basic level of independently assured security is required for the TOE.

EAL2 provides assurance by an analysis of the security functions, using a security-enforcing functional specification, guidance documentation, the basic design of the TOE to understand the security behavior. AVA_VAN.2 provides resistance against attackers with basic attack potential and ensures that the evidence shows that vulnerabilities have been analyzed. The analysis is supported by independent sample testing of the TOE security functions, evidence of developer testing based on the security-enforcing functional specification and basic design, selective independent confirmation of the developer test results, and a vulnerability analysis demonstrating resistance to penetration attackers with a basic attack potential.

7 TOE summary specification

This chapter presents an overview of the security functionality implemented by the TOE.

7.1 SF1 – Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. This function helps the authenticated user to find and fix MaxPatrol defects and misconfigurations.

All actions performed by TOE users that are listed in Table 6.2, except the operations view and use, are recorded by the Security Audit function. Further all authentication attempts regardless whether those were successful or failed are recorded. Within each log entry the following information is stored:

- Severity level (Critical, Error, Warning, Information or Debug),
- ID – event identification number,
- Date and Time – the date and time when the event occurred,
- Event type – the type of the event,
- Source – the system part which generated the event,
- Description – event details.

The Security Audit function logs within the description of the event the ID of the user who caused the event and the corresponding action performed by the user. In addition the outcome of the event (success or failure) is stored within the description (FAU_GEN.1, FAU_GEN.2).

Only authenticated users[10] are allowed to review the MP System security audit log. For a better finding of special events the user has the possibility to filter the stored events (FAU_SAR.1, FAU_SAR.2).

7.2 SF2 – Access Control

The TOE provides a Role-based access control policy to control the access of users to objects, based on the membership of this user to groups, the requested operation and the requested object (FDP_ACC.1).

Each identified and authenticated TOE user is a member of a user group which is associated with exactly one role. The user rights depend on the user group, since all members of a user group have the same rights. It is not possible to change the access rights of one specific user but only for a whole user group. Especially a new user can be assigned only to an already existing user group.

When a user attempts to perform an action to an object under the control of the TOE, the TOE decides whether the action is to be permitted based on the following rules (FDP_ACF.1):

- If the requested operation on the requested object is permitted to the group of which the authenticated user is a member, access will be grant,

[10] All users who were successfully identified and authenticated are allowed to review the audit log.

- else the access will be denied.

Within the certified version of the MaxPatrol Compliance and Vulnerability Management System the following roles are considered (FMT_SMR.1):

- Administrator – The members of the group that is associated with this role have unrestricted access to all TOE functionalities except of passwords of TOE users or accounts that are used to scan the scanned devices. Especially only the members of this group are allowed to create, remove and change users, user groups and object owners.
- Manager – The members of the group that is associated with this role are allowed to view the scanning results as well as to create reports and specify the delivery of the reports.
- Operator – The members of the group that is associated with this role are responsible for the scanning processes and able to use the predefined tasks.
- IT-Administrator – The members of the group that is associated with this role are only allowed to change and create the accounts that are necessary to access the scanned devices.

Table 6.2 provides a detailed overview of the allowed operations on objects by the different roles and therefore user groups.

Within the installation process the Administrator has to ensure that only the above listed user groups are in place and provide the corresponding access rights to the user groups correctly. Thereby the TOE provides restrictive default values for security attributes that are not allowed to change by any user of the TOE (FMT_MSA.3).

7.3 SF3 – Security Management

Security management specifies how the TOE allows managing the security functionalities of the TOE. This comprises the following management functions (FMT_SMF.1):

- View and edit the server settings,
- View and edit the inter server communications,
- Create, delete, edit and view users and user groups,
- Create, delete, edit, start and view tasks regarding the scanning process,
- Pause, cancel, continue and view active scans,
- Create, delete, edit, use and view the accounts that are necessary to access the scanned devices,
- Create, delete, edit, use and view the dictionaries that configure the logging function of the TOE,
- Create, delete, edit, use and view profiles which define the scanning parameters,
- Create, delete, edit, use and view compliances used for the analysis of the scanned devices,
- Create, delete, edit, start, cancel, pause, continue and view the schedules regarding the scanning process,

- Create, delete, edit, generate and view the reports that summarizes the scanning and analysis results,
- Create, delete, edit, use and view the delivery configurations for the reports,
- Create, delete, edit, use and view the overrides for variables,
- Edit and view the scanning results,
- Create, delete, edit, use and view the identification rules.

The management functions cannot be performed by all authenticated users but are assigned to authorized user roles. Those user roles are represented by user groups whereby each authenticated TOE user is a member of exactly one user group. Table 6.2 provides a detailed overview which management function can be performed by which user role (FMT_MSA.1, FMT_MTD.1).

To manage the TOE authorized users have to use the MP Console which is a graphical user interface.

7.4 SF4 – Scanning and Reporting

The Scanning and Reporting function performs the collection of system data of the scanned devices, analysis of the collected data, and generation of reports based on the analysis. For the scanning and analysis functionality the TOE differentiates between three different modes (EXT_SCR_SDC.1, EXT_SCR_ANL.1):

- PenTest – Network scanning
- Audit – System scanning
- Compliance – Compliance control

The scanning within the PenTest mode is provided using a minimum set of privileges on the scanned device. The purpose of this mode is to obtain the security assessment by an external attacker. Therefore the TOE has to identify vulnerabilities concerning server the network services and web applications. Furthermore the strength of password is checked by performing brute force attacks. The following activities are performed within the PenTest scanning mode:

- Identification of network services that uses the protocols TCP or UDP,
- Identification of vulnerabilities concerning the identified services,
- Analysis of the password strength by performing brute force attacks,
- Identification of the operating system.

The aim of the Audit mode is to get an overview of the security level of the scanned system from the perspective of a local user. Therefore the TOE uses the accounts maintained by the IT-Administrator to get access to the scanned devices. The following activities can be performed within the Audit scanning mode:

- Identification of the installed software and security updates,
- Identification of the remaining software vulnerabilities (with respect to security updates installed)
- Identification of the hardware including information about
    - Processor,

    - RAM,
    - BIOS,
    - Motherboard, and
    - Network interface card.
- Within the scanning of the Active Directory the following information shall be provided
    - Domain name of the server,
    - List of the domain users,
    - List of the domain groups.
- Within the scanning of Windows operation systems the following information shall be provided
    - List of the system services,
    - list of the Local user accounts,
    - list of the Local user groups,
    - list of connected printers, and
    - list of all accessible resources.

Within the Compliance mode the configuration of the scanned network and/or the scanned system are checked against predefined security and technical standards stored within the knowledge base[11]. Similarly to the Audit mode in Compliance mode the TOE uses the accounts maintained by the IT-Administrator to get access to the scanned devices.

Within the scanning process a scan document is created for each scan. This document contains unprocessed detailed data about scan results; the data is not grouped or filtered. The scan document is dynamically updated while the system is scanning (EXT_SCR_SDC.1).

Within the PenTest mode the following information is stored within the scanning results:

- Date and Time when the scan was performed,
- data concerning the scanned nodes (IP address, hostname, FQDN, etc.),
- open ports, protocols and services that are used within the network,
- identified vulnerabilities including the severity level according to CVSS and the recommendation how the vulnerability can be removed, and
- identified version of the operating system.

Within the Audit mode the scanning results contains the following information:

- Date and Time when the scan was performed,
- data concerning the scanned nodes (IP address, hostname, FQDN, MAC, etc.),
- identified vulnerabilities,
- identified version of the operating system, and
- data concerning the used hardware and software.

The scanning results for the Compliance mode consist of the following information:

- Date and Time when the scan was performed,
- data concerning the scanned nodes (IP address, hostname, FQDN),
- information whether the scanned system/network is compliant to predefined standards,

[11] Please note that the knowledge base is part of the MP Server but not of the TOE.

and

- recommendations how to achieve the security standard.

To perform a scanning process the authorized user has to create or use a task, define the scanning hosts, configure or use a profile and initiate the scanning process.

In most cases, data received after a single scan is hard to use since the data can be too detailed and the manner in which the data is organized significantly handicaps the analysis and comparison of information. Therefore reports can be used to process the scan data in a user-friendly structured format. To generate a report the authorized user (Administrator or Manager) creates a template that contains the parameters, which configure the content of the report and the data that should be considered within the report (EXT_SCR_RDR.1).

The TOE differentiates between five kinds of reports:

- Information report – report of a single scan,
- Differential report – report that highlights the difference between scanning results,
- Metric comparison report – report that defines how vulnerabilities were eliminated,
- Metric versus time report – report that shows the dynamics of vulnerabilities,
- Analytical report – compliance report considering the security standards.

The generated reports can be exported to network folders whereby the configuration is determined within the object “Deliveries”. Therefore the following parameters have to be set:

- Folder – name and path of the folder used to deliver the report,
- Authentication – user login and password to access the delivery folder,
- Report file name – name of the file, where the report is saved.

7.5 SF5 – Identification and Authentication

This security functionality requires each user to be successfully identified and authenticated before allowing any other actions on behalf of that user (FIA_UAU.2, FIA_UID.2).

The TOE provides the possibility to use two different identification and authentication mechanisms (FIA_UAU.5):

- MaxPatrol Authentication,
- Windows Authentication.

Within the creation of new users it is enforced that the authentication mechanism, the login credentials and the membership of a group is determined for that user (FIA_ATD.1).

When a user attempts to communicate with the TOE he has first of all to login to the TOE. If the flag “Login with current Windows credentials” is set, the Window Authentication mechanism is used, otherwise the MaxPatrol Authentication mechanism.

In case of Windows authentication the login is associated with a local or domain user account of the underlying Windows Operating System (FIA_ATD.1). For these logins the TOE requires that the Windows Operating System passes on the Windows credentials of that user to authenticate the user before any other action on behalf of that user is allowed. The verification of user name and password is therefore performed by the operational environment. The TOE attempts that the authentication mechanism provided by Windows Server 2008 R2 operates correctly.

The MaxPatrol authentication mechanism is maintained by the TOE itself. For every MaxPatrol Authentication login the TOE maintains a login name and a password. The password is not stored in plain text, but hashed using the SHA-1 hash function provided by the underlying operating system (FIA_ATD.1).

Each MaxPatrol Authentication login name and the corresponding hash of the password are stored in a table within the connected database.

If a user is connecting to the TOE using the MaxPatrol Authentication the user has to provide the username and password. The password is hashed by the underlying operating system and the hash is forwarded to the TOE. The TOE compares the hash to the value stored for that user in the database. If the values are identical the TOE has successfully authenticated the user.

7.6 Rationale on TOE specification

The specification of the TOE security functions refers directly to the TOE security requirements. The following table displays the correlation between security requirements and security functions.

Table 7.1 – Security Requirements vs. Security Functions

Security Requirements vs. Security Functions	**Security Audit**	**Access Control**	**Security Management**	**Scanning and Reporting**	**Identification and Authentication**
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FIA_ATD.1					X
FIA_UAU.2					X
FIA_UAU.5					X
FIA_UID.2					X
FDP_ACC.1		X			

Security Requirements vs. Security Functions	Security Audit	Access Control	Security Management	Scanning and Reporting	Identification and Authentication
FDP_ACF.1		X			
FMT_MSA.1			X		
FMT_MSA.3		X			
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1		X			
EXT_SCR_ANL.1				X	
EXT_SCR_SDC.1				X	
EXT_SCR_RDR.1				X	

8 Appendix

8.1 References

[CC] *Common Criteria for Information Technology Security Evaluation*, version 3.1, revision 4
Part 1: Introduction and general model, CCMB-2012-09-001*,*
Part 2: Security functional requirements, CCMB-2012-09-002*,*
Part 3: Security Assurance Requirements, CCMB-2012-09-003.

8.2 Acronyms

BIOS	Basic Input Output System
BSI	Bundesamt für Sicherheit in der Informationstechnik (German)
CC	Common Criteria
CVSS	Common Vulnerability Scoring System
DB	Database
EAL	Evaluation Assurance Level
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
MP	MaxPatrol
n/a	not applicable
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol