BMC® Real End User Experience Monitoring and Analytics 2.5

Security Target

Version 0.07

5 March 2015

bmcsoftware
BUSINESS RUNS ON I.T.™

Restricted Rights Legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 City West Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Document Revision History

Date	Revision	Author	Changes made
7 January 2014	0.01	TM	Initial Draft.
28 April 2014	0.02	TM	Addressed evaluator's comments
22 July 2014	0.03	TM	Addressed evaluator's comments
4 September 2014	0.04	TM	Addressed certifier's comments
18 September 2014	0.05	TM	Addressed evaluator's comments
3 October 2014	0.06	Chris Morris	Corrected build number
5 March 2015	0.07	TM	Clarification of syslog/SNMP

TABLE OF CONTENTS

1 SECURITY TARGET INTRODUCTION

This section presents Security Target (ST) identification information and an overview of the ST for *BMC Real End User Experience Monitoring and Analytics 2.5* (hereinafter referred to as *BMC EUEM*).

An ST contains the information technology (IT) 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. An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (TOE Security Environment section).
- A set of security objectives and a set of security requirements to address the security problem (Security Objectives and IT Security Requirements sections, respectively).
- The IT security functions provided by the TOE that meet the set of requirements in the TOE Summary Specification section.

The structure and content of this ST comply with the requirements specified in Annex A Specification of Security Targets of [CCP1] and Section 11 Class ASE: Security Target evaluation of [CCP3].

1.1 ST Reference

ST Title:	BMC Real End User Experience Monitoring and Analytics 2.5 Security Target
ST Version:	Version 0.07
ST Date:	5 March 2015

1.2 TOE Reference

TOE Identification:	BMC Real End User Experience Monitoring and Analytics 2.5
TOE Developer	BMC Software, Inc.
TOE Type	Application Performance Management

1.3 Document References

The following references are used in this ST:

Abbreviation	Document
[CC]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012, CCMB-2012-09-(001 to 003)
[CCP1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, July 2012
[CCP2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[CCP3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

1.4 Document Conventions

Section 8.1 in [CCP1] defines the approved set of operations that can be applied to the CC functional and assurance components: *assignment, refinement*, *selection,* and *iteration.* In this ST, these operations are indicated as follows:

1) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value] indicates an assignment. In the case when an assignment operation is embedded in a selection operation, the operations will be denoted as follows: *selection value [assignment_value]*.

2) The refinement operation is used to add detail or refine a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text** for new text and ~~strikethrough text~~ for deleted text.

3) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

4) Iterated security functional requirements will be identified by appending an additional identifier in round brackets next to their original identifier. For example: FMT_MTD.1(1) and FMT_MTD.1(2).

1.5 Document Terminology

1.5.1 CC Terminology

In the CC, many terms are defined in Section 4.1 of [CCP1]. The following terms are a subset of those definitions:

Term	Definition
Authentication data	The information used to verify the claimed identity of a user.
Authorized user	A TOE user who may, in accordance with the SFRs, perform an operation.
External entity	A human or IT entity possibly interacting with the TOE from outside of the TOE boundary.
Identity	A representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Operation (on an object)	A specific type of action performed by a subject on an object.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Security function policy	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of an intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.
Security requirement	A requirement, stated in a standardised language, which is meant to contribute to achieving the security objectives for a TOE.
Subject	An active entity in the TOE that performs operations on objects.
Target of evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE security functionality	The combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
TSF interface	The means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.
User	See external entity defined above.

1.5.2 Abbreviations

The following acronyms are used in this ST:

Term	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CSV	Comma Separated Variable
EAL	Evaluation Assurance Level
HTTP	Hyper Text Transfer Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NAS	Network Attached Storage
OSP	Organizational Security Policy
OVF	Open Virtualization Format
PAE	BMC Performance Analytics Engine
PCL	Performance Compliance Level
RBAC	Role-Based Access Control
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
URL	Uniform Resource Locator

1.6 TOE Overview

1.6.1 BMC Real End User Experience Monitoring and Analytics 2.5

The TOE is the BMC Real End User Experience Monitoring and Analytics (EUEM) 2.5, a system that monitors Web traffic (a data stream across a digital network between a client computer and a Web server). In Web-based applications, the user's browser software sends requests to a Web server using the Hypertext Transfer Protocol (HTTP). The Web server responds with the pages, images, and other documents the browser requested. Each request and its corresponding response contain a great deal of information; put together, the result of these individual requests is a Web page. Web protocols have no direct concept of pages and sessions, so the system must use clues and rules to reassemble several objects into a page, and string pages into user sessions. To do this, the system looks at page composition, and tries to identify sessions, users, time-outs, and departures.

1.6.1.1 Sessions

A session is an identifiable period of interaction between a Web user and one or more pages, whose duration is measured from the starting point of the interaction until either a certain amount of time passes since the user's last request or the user positively terminates the session (for example, via a logout action). To identify a session, most applications insert a unique string into the communication with a visitor. This is usually done with a cookie, which keeps track of the user's interaction and associates requests with shopping carts and accounts. The system can monitor cookies, keeping track of a user's session. Users don't tell the system when they have left a site, so it must wait for a certain amount of inactivity before it can declare a session terminated. Similarly, for slow pages the system might want to force the ending of a page rather than wait for the remaining components to be delivered.

1.6.1.2 Pages

In Web-based applications, the user's browser software sends requests to a Web server using HTTP. The Web server responds with the pages, images, and other documents the browser requested. Each request and its corresponding response contain a great deal of information; put together, the result of these individual requests is a Web page. A page is a set of objects consisting of the container object (for example, *.asp and *.jsp) and its subordinate frames and objects. The reference Uniform Resource Locator (URL) of the subordinate frames and objects is that of the container object.

1.6.1.3 Objects

Some objects (index.html, for example) are containers that encompass a page's content and layout. Other objects image.gif, style.css, script.js, for example) are components that are part of a page. Finally, some objects (document.pdf, file.zip, for example) stand alone; they are neither a container nor a component.

1.6.2 Data Collection and Analysis

BMC EUEM separates traffic capture from data analysis and presentation. This allows the system to consolidate data from multiple locations, providing:

- A single view of applications running in more than one data center
- The ability to follow user sessions when they move to another data center
- Comparison of application health and performance when served from multiple locations

A BMC EUEM system consists of at least one Collector device supplying data to at least one Analyzer device.

1.6.2.1 Real User Collector

Real User Collector devices capture traffic passing between the Web applications and end users via a network tap or mirror port on a switch or load balancer. Traffic Inclusion and Exclusion Policies allow control over what application data is captured. Using uploaded Secure Sockets Layer (SSL) keys, the Real User Collector device can decipher encrypted traffic. It can also obfuscate or delete private data. The flow of traffic into the device may be monitored via status information.

1.6.2.2 Real User Analyzer

Real User Analyzer devices continuously retrieve data from one or more Real User Collector devices. The data that the Real User Analyzer device consumes from a given Real User Collector device may be controlled by setting filters for each Collector feed. Feeds may be prioritized so that the most important data is available to 'dashlets', Collector feed reports, and other BMC EUEM monitoring features.

1.6.2.3 Performance Analytics Engine

The Performance Analytics Engine (PAE) provides additional analysis to that performed by the Real User Analyzer. The PAE stores traffic data and identifies the root cause of problems by using queries, summary views, and investigation of deeper levels of hierarchical performance data based on proprietary intelligence.

1.6.2.4 Watchpoints

The system passively monitors all the traffic to one or more Web applications. To make it easier to monitor only the parts of the Web traffic that are of interest, the system permits administrators to define precise segments of Web traffic, known as 'Watchpoints', which may be monitored in detail. Below are some examples of traffic segments for which Watchpoints may be defined:

- Traffic to a particular Web application
- Traffic from a particular group of end-users
- Traffic from a particular geographic region
- Traffic involving a particular part of the infrastructure
- Traffic from a particular client platform

For each Watchpoint, the system aggregates traffic volume, availability, and performance statistics in five minute intervals. Performance is the measure of how well a server or application instance is functioning, as measured by metrics such as availability, Page-render time, and throughput. Availability is a server's ability to share its resources as intended.

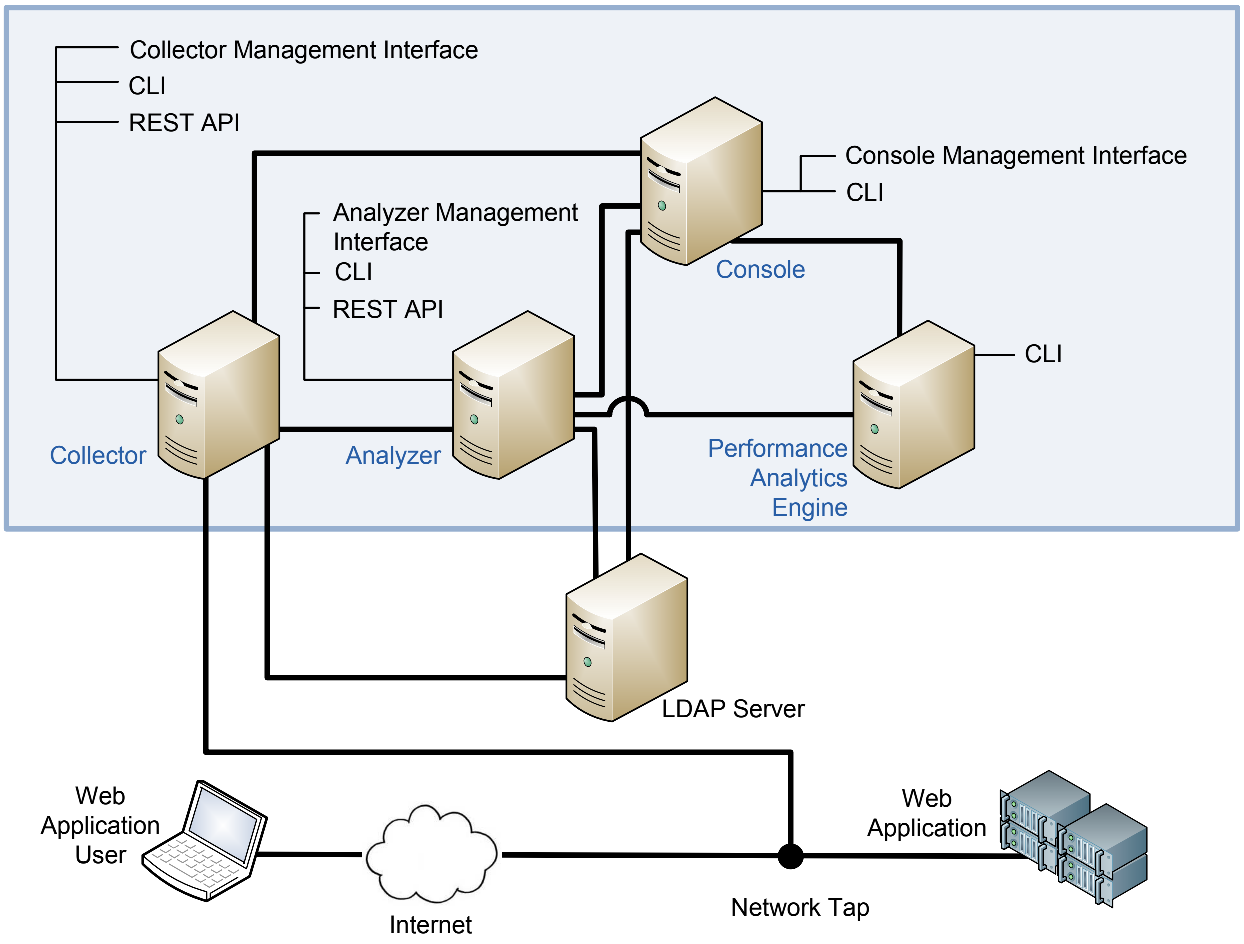
1.7 TOE Description

The following table identifies the BMC Real End User Monitoring and Analytics (also BMC EUEM in this ST) components and versions included in the evaluated configuration. The "abbreviated name" is used in this Security Target for discussion purposes.

Table 1 – BMC Real End User Monitoring component names, model and versions

BMC Real End User Monitoring component name	Version	Abbreviated name
BMC Application Performance Management Console	2.5.01 build 2.5.66.300	*Console*
BMC Real User Collector	2.5.01 build 2.5.66.300	*Collector*
BMC Real User Analyzer	2.5.01 build 2.5.66.300	*Analyzer*
BMC Performance Analytics Engine	2.5.01 build 2.5.66.300	*PAE*

Figure 1– BMC Real End User Experience Monitoring and Analytics TOE Boundary



1.7.1 Physical scope and boundary

Figure 1 illustrates the relationship between the major components of the BMC EUEM in the evaluated configuration of the TOE. The EUEM components are installed on VMWare servers. The components are deployed onto a Linux Kernel-based Virtual Machine using an ISO image file, or may be deployed via the VMware vSphere client using an Open Virtualization Format (OVF) template. A Management Computer is required to access the various interfaces. This computer, although required, is not shown in Figure 1.

1.7.1.1 BMC Real End User Monitoring Components

1.7.1.1.1 BMC Application Performance Management Console (Console)

The BMC Application Performance Console is the main user interface of the BMC EUEM. It hosts dashboards and system-management features. It also provides links to the user interfaces of the Analyzer and Collector components. The software is installed on the console and may be accessed from a web browser.

1.7.1.1.2 BMC Real User Collector (Collector)

The Collector captures traffic data from a tapping point between the application and the end user (the network tap) and makes it available to an Analyzer component. The Collector is responsible for deciphering the traffic and applying rules to protect the privacy of application end users. The Collector also has controls for managing a portion of its functionality.

1.7.1.1.3 BMC Real User Analyzer (Analyzer)

The Analyzer organizes into segments traffic data acquired from the Collector component, processes it, and provides usable information in various formats:

- Dashboards
- Reports incident detection features
- Session, page, and object statistics
- Data export functions

The Analyzer also has controls for managing a portion of its functionality.

1.7.1.1.4 BMC Performance Analytics Engine (PAE)

The BMC Performance Analytics Engine enables the storage of traffic data in a central, off-board storage location, and to locate the root cause of problems by sorting and filtering data.

1.7.1.2 Operational Environment

1.7.1.2.1 Admin Web Browser

A web browser will be used by Administrators and Users of the BMC EUEM to access the Console.

1.7.1.2.2 Network Tap

A network tap copies traffic for the purpose of monitoring. It is a passive device that, if it breaks, does not interrupt network traffic or the functioning of the application. A "smart" tap with the ability to filter on IP addresses and port numbers may also be used.

1.7.1.2.3 LDAP Server

When configured, an LDAP Directory Server is used to support user authentication.

1.7.1.3 Guidance Documentation

The TOE includes the following guidance documentation:

- BMC Real End User Experience Monitoring 2.5 20 Feb 2014

This document covers both installation and operation of the BMC EUEM.

1.7.2 Hardware and Software Requirements

The hardware requirements for any given environment depend on the size and amount of activity expected. This section describes the requirements used for the purposes of this evaluation.

1.7.2.1 TOE Component Requirements

The following table identifies the operating system and hardware required to support the TOE.

Table 2 – TOE Supporting Hardware and Software

TOE Component	Operating System	Hardware
Console	ESXi 5.5	General Purpose VMWare supported server platform
Analyzer	ESXi 5.5	General Purpose VMWare supported server platform

TOE Component	Operating System	Hardware
Collector	ESXi 5.5	General Purpose VMWare supported server platform
Performance Analytics Engine	ESXi 5.5	General Purpose VMWare supported server platform

The following table identifies other components in the operational environment required to support the TOE.

Table 3 – Operational Environment Hardware and Software

Environment Component	Supported Product
Web Browser	Google Chrome
LDAP Server	General purpose hardware with any LDAP supporting operating system

1.7.3 Logical scope and boundary

The TOE provides the following security functions:

- Security audit
- User data protection
- Identification and authentication
- Security management
- User session data collection and reporting

1.7.3.1 Security Audit

The TOE logs events related to user log in and security management.

A user can log on the Console, Analyzer or Collector components using their web interface. Logs are stored on the component where the action is performed.

1.7.3.2 User Data Protection

The TOE enforces a Role Based Access Control (RBAC) Policy to restrict access to the management functions of the TOE based on roles.

1.7.3.3 Identification and Authentication

The TOE requires users to provide unique identification and authentication data prior to being granted any administrative access to the system. The TOE maintains username and role information for each user, and password information for each locally-authenticated user. Password policy is enforced for locally authenticated users when a user logs in.

The BMC EUEM requires users to provide unique identification and authentication data prior to being granted any administrative access to the system. The TOE enforces a RBAC Policy, which restricts access to the management functions of the TOE. This protection requires that users of the TOE must be authenticated prior to granting access to the management functions.

1.7.3.4 Security Management

Security management functionality is provided through the Management Console and through the Command Line Interface (CLI) on the component being managed. Functionality is provided to support configuration, user management, configure monitoring of web traffic, analyze that traffic and provide detailed reports.

1.7.3.5 User Session Data Collection and Reporting

The TOE will provide functionality to automatically capture user sessions in real time, analyze the data and report on errors and performance issues related to the end user experience.

1.7.4 Functionality Excluded from the Evaluated TOE

The following are excluded from this evaluation:

- Cloud Probe
- Real User Monitor
- TrueSight Hardware
- Syslog Server interface
- SNMP Monitor interface
- Mail Server interface
- BMC Synthetic End User Experience Monitoring
- Content-delivery network visibility
- Rich internet application visibility
- Use of Secure Shell (SSH) with the CLI
- Integration with OpenLDAP (slapd) and Oracle Application Server for LDAP authentication
- Integration with the following other BMC products:
  - BMC ProactiveNet Performance Management
  - BMC Application Diagnostics
  - BMC Atrium Configuration Management Database
  - BMC Transaction Management Application Response Time
  - BMC Service Level Management
  - BMC Patrol

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

This Security Target claims to be conformant to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CCP1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CCP2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CCP3]

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 [CEM] has to be taken into account.

2.2 Protection Profile Claim

This Security Target does not claim conformance to a validated Protection Profile.

2.3 Assurance Package Claim

This Security Target claims conformance to Evaluation Assurance Level 2+ augmented with ALC_FLR.2.

3 SECURITY PROBLEM DEFINITION

3.1 Threats

Table 11 lists threats to the resources to be protected by the TOE. The threat agents to the TOE are considered to be unauthorized users with public knowledge of how the TOE operates and who possess the skills and resources to alter TOE configuration settings, or parameters, or both. The threat agents do not have physical access to the TOE. Mitigation to the threats is through the objectives identified in Section 4.1 Security Objectives.

Table 4 – Threats

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.PERFORM	Administrators may be unaware of the errors resulting from network and application issues that end users receive while using their web applications. This leads to negative user experience, customer attrition, and revenue risk.
T.UNAUTH	A hostile/unauthorized user may be able to read TOE data/configuration files in order to ascertain TOE or monitored application secrets, or modify TOE behavior.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

3.2 Organizational Security Policies

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. Table 11 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

Table 5 – Organizational Security Policy

Threat	Description
P.MANAGE	The TOE must provide the functions to facilitate effective management.

3.3 Assumptions

The assumptions are delineated in Table 12 are required to ensure the security of the TOE:

Table 6 – Assumptions

Assumptions	Description
A.ADMIN	One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
A.NOEVIL	Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.

Assumptions	Description
A.PHYSICAL	The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical and network access.
A.TIME	The operational environment will provide reliable system time.

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address all of the security concerns, and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats can be directed against the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives for the TOE, as shown in Table 13.

Table 7 – Security objectives for the TOE

Security Objective	Description
O.ACCESS	The TSF must limit access to objects maintained by the TOE to users or applications with authorization and appropriate privileges. The TSF must provide the functions to specify which users may access objects and which actions may be performed on the objects.
O.MONITOR	The TSF must proactively detect and isolate end-user performance issues before they negatively impact business reputation and revenue.
O.AUTH	The TSF must ensure that only authorized users and applications gain access to the TOE and its resources.
O.AUDIT	The TSF must ensure that requests to invoke controlled interfaces are audited so that those users can be held accountable for their actions.
O.MANAGE	The TSF must provide all of the functions and facilities necessary to support the Authorized Administrators that are responsible for the management of TOE security.

4.2 Security Objectives for the Environment

This section identifies and describes the security objectives for the environment, as shown in Table 14.

Table 8 – Security objectives for the environment

Objective	Description
OE.ADMIN	One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
OE.NOEVIL	All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.
OE.PHYSICAL	The TOE will be located within controlled access facilities that will prevent unauthorized physical access. Those responsible for the TOE must ensure that the host computer system(s) containing the TOE components are protected from physical attack.
OE.TIME	The TOE operational environment must provide reliable system time to the TOE.

4.3 Security Objectives Rationale

This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered by the TOE, and that all objectives for the environment are traced back to assumptions for the environments.

Table 9 – Security objective to threats and OSP correspondence

	Threats and OSPs				
	T.ACCOUNT	T.PERFORM	T.UNAUTH	T.UNDETECT	P.MANAGE
O.ACCESS	X				
O.MONITOR		X			
O.AUTH			X		
O.AUDIT				X	
O.MANAGE					X
OE.ADMIN					
OE.LOCATE					
OE.LOCK_DOWN					
OE.NOEVIL					
OE.PHYSICAL					
OE.TIME					

Table 10 – Security objective to threats and assumptions correspondence

	Assumptions			
	A.ADMIN	A.NOEVIL	A.PHYSICAL	A.TIME
O.ACCESS				
O.MONITOR				
O.AUTH				
O.AUDIT				
O.MANAGE				
OE.ADMIN	X			
OE.NOEVIL		X		
OE.PHYSICAL			X	
OE.TIME				X

Table 11 – Security objectives rationale for the TOE

Objective	Threat	Rationale
O.ACCESS	T.ACCOUNT	O.ACCESS mitigates the T.ACCOUNT threat by limiting access to TOE objects.
O.MONITOR	T.PERFORM	O.MONITOR mitigates the threat T.PERFORM by proactively detecting and isolating end-user performance issues before they negatively impact business reputation and revenue.
O.AUTH	T.UNAUTH	O.AUTH helps to mitigate the threat T.UNAUTH by requiring the TOE to allow only authorized users and applications access to the TOE.
O.AUDIT	T.UNDETECT	O.AUDIT mitigates the threat T.UNDETECT by ensuring that requests to invoke TOE functions accessed through controlled interfaces are recorded.
O.MANAGE	P.MANAGE	O.MANAGE supports the OSP P.MANAGE by providing all of the functions and facilities necessary to support authorized administrators responsible for management of TOE security.

Table 12 – Environment security objectives rationale for the TOE

Objective	Assumption	Rationale
OE.ADMIN	A.ADMIN	OE.ADMIN maps to A.ADMIN in order to ensure that authorized administrators install, manage and operate the TOE in a manner that maintains its security objectives.
OE.NOEVIL	A.NOEVIL	OE.NOEVIL directly maps to A.NOEVIL and ensures that all users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided.
OE.PHYSICAL	A.PHYSICAL	OE.PHYSICAL meets the environmental assumption A.PHYSICAL by requiring that the TOE be located within facilities providing controlled access, to prevent unauthorized physical access. OE.PHYSICAL ensures that those responsible for the TOE locate the TOE in a controlled access facility that will prevent unauthorized physical access.
OE.TIME	A.TIME	OE.TIME meets the assumption A.TIME by requiring that the operational environment of the TOE provide reliable system time to the TOE.

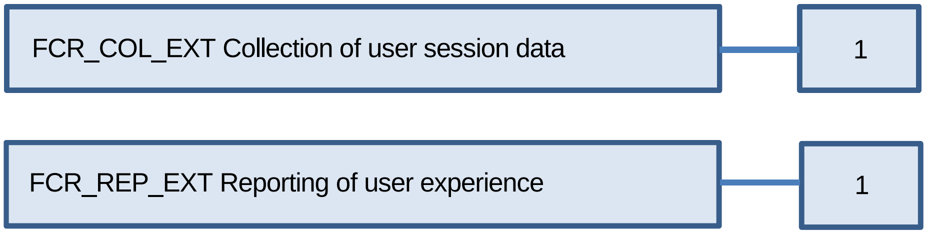
5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFRs) used in this ST.

5.1 Class FCR User session data collection and reporting

The User session data collection and reporting class addresses the collection and reporting of data used to identify potential problems associated with an end user's web session experience. The class is modeled on the FAU Security Audit class. Two families, Collection of user session data and Reporting of user experience, are defined for this class. Both families are modeled after FAU_GEN Security audit data generation. FCR_COL_EXT.1 was modeled after FAU_GEN.1, and FCR_REP_EXT.1 was modeled after FAU_SAR.1. Component leveling is shown in Figure 2 below.

Figure 2– Component Leveling


FCR_COL_EXT Collection of user session data
1
FCR_REP_EXT Reporting of user experience
1

5.1.1 Collection and Analysis of user session data (FCR_COL_EXT.1)

Family Behavior: This family defines a requirement for ensuring that the TOE automatically captures user session data in real time and performs analysis on the captured data in order to identify the root cause of network problems.

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

- Configure monitoring activities.

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

- Basic: Administrator changes to monitoring activities.

FCR_COL_EXT.1	**Collection of user session data**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCR_COL_EXT.1 .1	The TSF shall be able to automatically capture user sessions in real-time and perform analysis on the captured data.

5.1.2 Reporting of end user experience (FCR_REP_EXT.1)

Family Behavior: This family defines a requirement for ensuring that the TOE reports on errors and performance issues related to the end user experience.

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

- Produce reports.

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

- There are no auditable events foreseen.

FCR_REP_EXT.1	**Reporting of end user experience**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCR_REP_EXT.1 .1	The TSF shall be able to report on errors and performance issues that end users experience when using a monitored web application.

5.2 Rationale for the Extended TOE Security Functional Components

FCR_COL_EXT.1 and FCR_REP_EXT.1 were created to capture the basic functionality provide by the TOE.

5.3 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6 SECURITY REQUIREMENTS

6.1 Security Functional Requirements

The table provided below is a summary of the operations performed on the security functional requirements selected for the TOE. The operations will be identified as follows: A = Assignment, S = Selection, R = Refinement and I = Iteration.

Table 13 – TOE security functional requirements

Class	Functional component	A	S	R	I
Security Audit (FAU)	**FAU_GEN.1** Audit data generation	X	X		
	FAU_GEN.2 User identity association				
User Data Protection (FDP)	**FDP_ACC.1** Subset access control	X			
	FDP_ACF.1 Security attribute based access control	X			
Identification and Authentication (FIA)	**FIA_ATD.1** User attribute definition	X			
	FIA_SOS.1 Verification of secrets	X			
	FIA_UAU.2 User authentication before any action				
	FIA_UAU.5 Multiple authentication mechanisms	X			
	FIA_UID.2 User identification before any action				
Security Management (FMT)	**FMT_MOF.1** Management of security functions behaviour	X	X		
	FMT_MSA.1 Management of security attributes	X	X		
	FMT_MSA.3 Static attribute initialization	X	X		
	FMT_MTD.1 Management of TSF data	X	X		
	FMT_SMF.1 Specification of Management Functions	X			
	FMT_SMR.1 Security roles	X			
User session data collection and reporting (FCR)	**FCR_COL_EXT.1** Collection of user session data				
	FCR_REP_EXT.1 Reporting of end user experience				

6.1.1 Security Audit (FAU)

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) [user login].
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, [no other information].

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.

6.1.2 User Data Protection (FDP)

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 SFP] on [subjects: system users objects: system data operations: system functions].

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 SFP] to objects based on the following: [subject: system user subject attributes: role objects: system data object attributes: none].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the user is allowed access to the system data if the user is authenticated and the assigned role specifies access to the functions that require access to that data].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

Application Note: For the purposes of FDP_ACC.1 and FDP_ACF.1, ‘system data’ refers to the data required to modify security settings, user accounts, and system configuration.

6.1.3 Identification and Authentication (FIA)

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 name, role].

FIA_SOS.1	**Verification of secrets**
Hierarchical to:	No other components.

Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [passwords must have a minimum of 10 characters passwords must include two of the following special characters: 0 1 2 3 4 5 6 7 8 9 ~ ! @ # $ % ^ & * ( ) _ + - = the special characters must be noncontiguous].

Application Note: Password rules are enforced on local user accounts.

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 [local account and LDAP authentication] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [rules: a) if a valid local account username and password is provided to the TOE component; or b) if the associated LDAP server contains a valid account for the provided credentials].

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.

6.1.4 Security Management (FMT)

FMT_MOF.1	**Management of security functions behaviour**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to *determine the behaviour of* the functions [security settings, including private key management, enabling and disabling the traffic capture, and configuring data confidentiality polices] to [users associated with the Security Officer role].

Application Note: Within the TOE, ‘data confidentiality’ refers to data handling procedures, not cryptography.

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow 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 SFP] to restrict the ability to *query, modify, delete,[create]* the security attributes [account information] to [users assigned the Security Officer and Administrator role].

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 SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [users assigned the Security Officer or Administrator roles] 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_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [*perform the functions specified in Table 14 to*] the [data specified in Table 14] to [the roles specified in Table 14].

Table 14 – System Management Functions

Role(s)	Functions	Data
Security Officer	Query, Modify, Delete	Security policy data
Security Officer, Administrator	Create, Modify, Delete	User account data
Security Officer, Administrator, Operator	Query, Modify, Delete	Configuration data

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 management functions: [configure users, configure security settings, configure monitoring activities, configure analysis activities, and produce reports].

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 [Security Officer, Administrator, Operator, Observer, Export].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.5 FCR User session data collection and reporting

FCR_COL_EXT.1	**Collection of user session data**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCR_COL_EXT.1 .1	The TSF shall be able to automatically capture user sessions in real-time and perform analysis on the captured data.

FCR_REP_EXT.1	**Reporting of end user experience**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCR_REP_EXT.1 .1	The TSF shall be able to report on errors and performance issues that end users experience when using a monitored web application.

6.2 Security Assurance Requirements

The TOE satisfies the Security Assurance Requirements (SARs) delineated in Table 15.

Table 15 – TOE security assurance requirements

Class	Assurance Component
Development (ADV)	**ADV_ARC.1** Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Guidance Documents (AGD)	**AGD_OPE.1** Operational user guidance
	AGD_PRE.1 Preparative procedures
Life-Cycle Support (ALC)	**ALC_CMC.2** Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Security Target Evaluation (ASE)	**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
Tests (ATE)	**ATE_COV.1** Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Vulnerability Assessment (AVA)	**AVA_VAN.2** Vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following two tables provide the security requirement to security objective mapping and a rationale to justify the mapping.

Table 16 – Objective to requirement correspondence

	O.AUDIT	O. ACCESS	O.AUTH	O.MANAGE	O.MONITOR
FAU_GEN.1 Audit data generation	X				
FAU_GEN.2 User identity association	X				
FDP_ACC.1 Subset access control		X			
FDP_ACF.1 Security attribute based access control		X			
FIA_ATD.1 User attribute definition			X		
FIA_SOS.1 Verification of secrets			X		
FIA_UAU.2 User authentication before any action			X		
FIA_UAU.5 Multiple authentication mechanisms			X		
FIA_UID.2 User identification before any action			X		
FMT_MOF.1 Management of security functions behaviour				X	
FMT_MSA.1 Management of security attributes				X	
FMT_MSA.3 Static attribute initialization				X	
FMT_MTD.1 Management of TSF data				X	
FMT_SMF.1 Specification of Management Functions				X	
FMT_SMR.1 Security roles				X	
FCR_COL_EXT.1 Collection of user session data					X
FCR_REP_EXT.1 Reporting of end user experience					X

Table 17 – Security functional requirements rationale for the TOE

Objective	SFR	Rationale
O.AUDIT	**FAU_GEN.1**	FAU_GEN.1 defines the security relevant events that will be recorded by the TOE along with the details of the event that will be recorded.
	FAU_GEN.2	FAU_GEN.2 requires the TOE to associate each auditable event with the identity of the user that caused the event.
O.ACCESS	**FDP_ACC.1**	FDP_ACC.1 requires the TOE to prevent unauthorized access to TOE resources by enforcing the Role Based Access Control SFP.
	FDP_ACF.1	FDP_ACF.1 requires the TOE to enforce the Role Based Access Control SFP on the protected TOE resources.
O.AUTH	**FIA_ATD.1**	FIA_ATD.1 ensures that the TOE maintains the user information required to enforce identification and authentication policies.
	FIA_SOS.1	FIA_SOS.1 ensures that the TOE enforces password security policy.
	FIA_UID.2	FIA_UID.2 requires a user be identified before any access to the TOE and resources protected by the TOE is allowed.
	FIA_UAU.5	FIA_UAU.5 requires that the TOE provide multiple authentication mechanisms (local accounts and LDAP).

Objective	SFR	Rationale
	FIA_UID.2	FIA_UID.2 requires a user be identified before any access to the TOE and resources protected by the TOE is allowed.
O.MANAGE	**FMT_MOF.1**	FMT_MOF.1 allows users in the Security roles to manage the behavior of sensitive functions in the TSF.
	FMT_MSA.1	FMT_MSA.1 restricts the assignment of security attributes of users and resources to the authorized administrators.
	FMT_MSA.3	FMT_MSA.3 allows the authorized administrators to override the default values set for security attributes when creating user accounts.
	FMT_MTD.1	FMT_MTD.1 restricts access to sensitive TSF data according to user role.
	FMT_SMF.1	FMT_SMF.1 requires that the TOE provide the ability to manage its security functions including the management of user accounts, security settings and monitoring and analysis activities.
	FMT_SMR.1	FMT_SMR.1 requires the TOE to provide roles to restrict users to varying sets of functions.
O.MONITOR	**FCR_COL_EXT.1**	FCR_COL_EXT.1 ensures that the TOE provides the functionality to capture user session information.
	FCR_REP_EXT.1	FCR_REP_EXT.1 ensures that the TOE provides the functionality to report on errors and performance issues.

6.3.2 Rationale for SFR Dependencies

Table 23 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied, or provides justification for why the dependency was not satisfied.

Table 18 – SFR dependency status

SFR	Dependencies	Fulfilled by SFRs in this ST
FAU_GEN.1	FPT_STM.1	Timestamps are provided by the environment in accordance with the OE.TIME objective.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.2, which is hierarchical to FIA_UID.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
	FMT_MSA.3	FMT_MSA.3
FIA_ATD.1	None	Not applicable
FIA_SOS.1	None	Not applicable
FIA_UAU.2	FIA_UID.1	FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UAU.5	None	Not applicable
FIA_UID.2	None	Not applicable
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1

SFR	Dependencies	Fulfilled by SFRs in this ST
FMT_SMF.1	None	Not applicable
FMT_SMR.1	FIA_UID.1	FIA_UID.2, which is hierarchical to FIA_UID.1
FCR_COL_EXT.1	None	Not applicable
FCR_REP_EXT.1	None	Not applicable

6.3.3 Security Assurance Requirements Rationale

Evaluation Assurance Level (EAL) 2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile location and protected by other products designed to address threats that correspond with the intended environment. ALC_FLR.2 was added to provide assurance that the vendor will respond to reports of new threats and reported defects in the TOE.

7 TOE SUMMARY SPECIFICATION

7.1 Mapping of the TSFs to SFRs

The specified TSFs work together to satisfy the TOE SFRs. Table 19 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 19 – Mapping of TSFs to SFRs

TSF	SFR
Security Audit	**FAU_GEN.1** Audit data generation
	FAU_GEN.2 User identity association
User Data Protection	**FDP_ACC.1** Subset access control
	FDP_ACF.1 Security attribute based access control
Identification and Authentication	**FIA_ATD.1** User attribute definition
	FIA_SOS.1 Verification of Secret
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UID.2 User identification before any action
Security Management	**FMT_MOF.1** Management of security functions behaviour
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
User session data collection and reporting	**FCR_COL_EXT.1** Collection of user session data
	FCR_REP_EXT.1 Reporting of end user experience

7.2 Audit

The audit logs record each user access from any means (web access, CLI, Application Programming Interface (API) calls). Logs are stored on the component where the action is performed.

A range of logging messages may be sent to the log-collection system. The logging level designates the level of severity of the logs that are collected. In the evaluated configuration, this must be set to at least 'Informational' in order to record successful user login activities. 'Informational' is the second highest of the seven possible logging levels, as shown in Table 20. The syslogparams command is used through the CLI to set the logging level and the ip address where the logs are to be sent. The CLI may only be used to change this setting for the Console and PAE components. The UI must be used to make similar changes for the Collector and Analyzer components.

Table 20 – Logging Levels

Logging Level Number	Level Name	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately

Logging Level Number	Level Name	Description
2	Critical	Critical conditions exist
3	Error	Error conditions exist
4	Warning	Warning conditions exist
5	Notice	Normal but significant conditions exist
6	Informational	Informational messages
7	Debug	Debug-level messages

7.3 User Data Protection

The BMC EUEM enforces a Role Based Access Control (RBAC) Policy to restrict access to the management functions of the TOE based on roles, as described in Section 7.5. The TOE enforces access to the various functions based on the user's role. The Console, Analyzer and Collector components each maintain their own list of users and roles. The PAE does not maintain a list of users. Management controls for the Performance Analytics Engine component are provided through the Console; however, some configuration activities must be performed directly on the Performance Analytics Engine component using its CLI.

7.4 Identification and Authentication

The TOE requires users to provide unique identification and authentication data prior to being granted any administrative access to the system. The TOE enforces a Role Based Access Control Policy, which restricts access to the management functions of the TOE, as described in Section 7.5.

When local user authentication is used, the user account information is stored locally on the Console, Collector or Analyzer device. Each component maintains its own list of users and roles. When an LDAP Directory is used, the user is authenticated by the Directory service. Authorization may be performed locally, or through the LDAP Directory. If authorization is performed by the LDAP Directory, system roles must be mapped to LDAP groups associated with users. A default role may be mapped to all users authenticating using the LDAP Directory; however, this feature is not be used in the evaluated configuration.

For locally managed accounts, the user name must consist of 1 to 64 alphanumeric characters, but cannot contain the @ symbol. For LDAP accounts, the user name must follow the rules of the LDAP server.

For locally managed account, passwords are initially set by an Administrator and may be updated by the account owner. In the evaluated configuration, the 'strict password' rule is enabled. When the strict password rule is enabled, the system prompts users who try to log on with simple passwords to change their passwords.

A 'strict password' must have:

- A minimum of 10 characters
- Two noncontiguous nonalphabetic characters from the following set:
  0 1 2 3 4 5 6 7 8 9 ~ ! @ # $ % ^ & * ( ) _ + - =

Note that the TOE enforces password rules for passwords created on TOE components only, and not for passwords created on LDAP servers.

The BMC EUEM includes APIs that allow users to export data and configure features. The same credentials are used and the same Role Based Access Control Policy used for the web interface is enforced for use of the APIs.

Access to the CLI is protected by a password. There is a single user account[1] that may be used to access the CLI. In the evaluated configuration, access to this account may only be provided to users in the Security Officer or Administrator roles, and the default password for this account must be changed during installation.

7.5 Security Management

A web interface is provided by each of the Console, Analyzer and Collector components to perform security management activities. The Console is the primary access point to the system, and is used to perform the day-to-day tasks, such as monitoring performance on dashboards, running traffic-data queries, and managing system components and access. It is also used to access the PAE, which has no login page. The Console directs users to login pages for the Collector and Analyzer components. The Analyzer and Collector components provide the functionality to manage captured traffic, set up Collector feeds, configure Watchpoints, and access the Watchpoint Summary, Session Browser, Incidents, and Reports.

Some configuration functionality is provided through the CLI of each of the components (Console, Analyzer, Collector and PAE).

7.5.1 Web Interfaces

Permissions associated with the various roles are shown in Table 21.

Table 21 – User Permissions

Permission Role	Security Settings	Accounts	Overall Configuration	Web Interface Access	Data Download
Security Officer	x	x	x	x	x
Administrator		x	x	x	x
Operator			x	x	x
Observer				x	x
Export					x

Any of the following roles may be assigned to a user:

- Security Officer. This provides access to sensitive configurations, such as private key management, enabling and disabling the traffic capture, and configuring data confidentiality policies (on the Collector component).
- Administrator. Provides access to all functions of the system that are not related to security. This role exists primarily for account management purposes.
- Operator. Provides access to all features that the Administrator role has except for account management. This role exists for device and data management purposes.
- Observer. Provides access to the web interface, but users with this role cannot make any configuration changes other than to save or edit report settings and saved query settings. The permissions of this role are sufficient to perform day-to-day tasks.
- Export. Provides no access to the web interface and is limited to downloading data via data export APIs.

By default, no security attributes are included in the account information until added by the Security Officer or Administrator role administrator. These administrators may create default roles for new users when LDAP authentication is used.

[1] Due to legacy issues, the CLI system account may be accessed by the username clisystem or cliuser; however, only one password effectively applies to either user name.

7.5.2 Command Line Interface

Login to the CLI provides access to the following functions:

- Firmware upgrade
- System reboot and diagnostics
- Network parameters management
- Create a Security Officer

Access to traffic data is not permitted. There is a single user account that may be used to access the CLI. In the evaluated configuration, access to this account may only be provided to users in the Security Officer or Administrator roles, and the default password for this account must be changed during installation.

7.6 User session data collection, analysis and reporting

The BMC EUEM provides data collection through the Collector component, analysis through the Analyzer and Performance Management Engine components, and reporting through the Analyzer component.

7.6.1 Data Collection and Analysis

Collector devices capture traffic passing between web applications and end users via a network tap or mirror port on a switch or load balancer. Traffic Inclusion and Exclusion Policies provide control over the application data to be captured. The Collector may also obfuscate or delete private data. The flow of traffic into the device may be monitored via status information in the web interface.

Analyzer devices continuously retrieve data from one or more Collector devices. The data being collected may be controlled by setting filters for each Collector feed. Feeds may be prioritized to ensure that the most important data is available to be displayed in the panes of the web interface and in reports. The system passively monitors all the traffic to one or more Web applications. To monitor only the parts of the web traffic that are of interest, the system permits administrators to define precise segments of web traffic, known as Watchpoints, which may be monitored in detail. Examples of traffic segments for which Watchpoints would be defined are:

- Traffic to a particular web application
- Traffic from a particular group of end-users
- Traffic from a particular geographic region
- Traffic involving a particular part of the infrastructure
- Traffic from a particular client platform

For each Watchpoint, the system aggregates traffic volume, availability, and performance statistics in five minute intervals. Performance is the measure of how well a server or application instance is functioning, as measured by metrics such as availability, Page-render time, and throughput. Availability is a server's ability to share its resources as intended.

Further analysis is performed by the PAE component. It stores traffic data and identifies the root cause of problems by using queries, summary views, and investigation of deeper levels of hierarchical performance data based on proprietary intelligence.

7.6.2 Reporting

Reports are created in the Report library tab of the Analyzer interface, and may be viewed on screen or exported to a comma separated variable (CSV) file through the web interface. Reports provide the following types of performance analysis information:

- Service Level Threshold (SLT) analysis shows whether the current performance satisfies specific, configured service-level thresholds

- Trend analysis shows how performance degrades as traffic increases
- Application analysis shows application delivery, responsiveness, and redirects
- Network quality metric analysis can show how poor network quality affects performance
- Bandwidth analysis shows how much bandwidth the specified application takes
- Error analysis shows the most common kinds of errors for the monitored web application

The system supports both preconfigured and custom reports. Performance compliance reports compare performance for a metric over time with performance-compliance levels (PCLs) to display how many users the system characterizes as satisfied, tolerating, or frustrated within the specified time range. Performance compliance reports may also be used to learn the percentage of requests that were characterized as frustrated or tolerating. If there are customized PCLs for the Watchpoint being reported on, the chart compares requests to them. Otherwise, the performance compliance chart compares requests to the system-wide PCLs configured by an Administrator.

bmcsoftware

BUSINESS RUNS ON I.T.™