Hewlett Packard Enterprise Development LP
HP Universal CMDB and Universal Discovery v10.21

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.1

Prepared for:

Hewlett Packard Enterprise Development LP
3000 Hanover Street
Palo Alto, CA 94304
United States of America

Phone: +1 305 267 4220
Email: info@hpe.com
http://www.hpe.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Hewlett-Packard (HP) HP Universal CMDB and Universal Discovery v10.21, and will hereafter be referred to as the TOE throughout this document. The TOE discovers and collects data from the IT[1] network for various physical and logical entities. Physical entities consist of servers, network, and storage devices. Logical entities consist of business services, web applications, databases, VPNs[2], end users, SLAs[3], etc. Once the collected data is analyzed, TOE administrators can perform impact analyses on proposed configuration changes, policy management and enforcement, and change tracking and control.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	Hewlett Packard Enterprise Development LP HP Universal CMDB and Universal Discovery v10.21 Security Target
ST Version	Version 1.1
ST Author	Corsec Security, Inc.
ST Publication Date	3/11/2016

[1] IT – Information Technology
[2] VPN – Virtual Private Network
[3] SLA – Service Level Agreement

ST Title	Hewlett Packard Enterprise Development LP HP Universal CMDB and Universal Discovery v10.21 Security Target
TOE Reference	HP Universal CMDB and Universal Discovery
FIPS[4] 140-2 Status	Level 1, RSA[5] BSAFE Crypto-J JSAFE and JCE[6] Software Module, Software Version 6.1, Certificate No. 2057 Level 1, OpenSSL FIPS Object Module, Software Version 2.0.7, Certificate No. 1747

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, 1.4 TOE Overview, will introduce the parts of the overall product offering that are specifically being evaluated.

The HP UCMDB and UD solution's components form the foundation for HP's Configuration Management System (CMS). The HP CMS is capable of automatically collecting and managing business service definitions, management data repositories, IT infrastructure relationships, and detailed asset information. The collected data is used to provide a 'single version of truth', providing data to CMS users in a consistent and non-redundant form. The HP UCMDB and UD is composed of the UCMDB, UD, CM, and UCMDB Browser components; each plays a specialized role in the overall CMS and will be described in the following sections.

1.3.1 Universal Configuration Management Database

UCMDB is a central repository for storing configuration information gathered using the DFM[7] process as well as various third-party applications and tools. UCMDB reconciles data from multiple discovered and federated sources, also referred to as Configuration Items (CI), into a single data set. It models business services for an organization, calculates the potential impact that results due to changes within these services, tracks changes for any CI, and contains event-based reporting capabilities. UCMDB uses the collected data to create a shared 'single version of truth' to support business service management, IT service management, configuration change management, and asset management initiatives. It is the central component of the HP CMS.

At the core of the UCMDB is the UDM[8] that supports various physical and logical entities and the complex relationships between these entities. Each entity is a CI, and each CI is a member of a specific Configuration Item Type (CIT). CIT templates define categories of CIs that can be organized into a hierarchical format based on interdependencies, or relationships. Using the UCMDB Integration Studio, UCMDB administrators can manage replication and federation data flows from existing MDRs[9] and configure reconciliation rules based on a specific CIT. Reconciliation rules allow UCMDB to take action when the CI data arriving into the UCMDB does not match the expected configuration data as defined by the CIT.

The CIs and relationships can enter the UCMDB either through the automated DFM process or manual entry. To access the entities, UCMDB maintains the credentials in the Oracle 11g Databases. UCMDB encrypts all credentials prior to storage using an AES-192-bit encryption key to protect these credentials from unauthorized disclosure. These relationships represent a model of all IT infrastructure components and applications that drive business operations. CIs can be viewed and managed in UCMDB Integration

[4] FIPS – Federal Information Processing Standard
[5] RSA – Ron Rivest, Adi Shamir, and Leonard Adleman
[6] JCE – Java Cryptography Extension
[7] DFM – Data Flow Management
[8] UDM – Universal Data Model
[9] MDR – Management Data Repository

Studio using the 'views' feature, which collectively represents the "IT Universe" model. UCMDB stores and handles the infrastructure data collected and updated by the DFM process. All data within the UCMDB can be queried using Topology Query Language (TQL), which uses natural language queries to retrieve information in a user-friendly fashion.

UCMDB also supports multi-tenancy, which allows service providers and large distributed organizations to manage several tenants within a single instance of UCMDB. This provides flexibility in management of the data and security for both shared and non-shared data.

UCMDB provides robust access control through various permission types. "Resource Groups" allow resources such as TQL queries, views, reports, and correlation rules to be bundled together so that permissions may be managed as a single group. User permissions can also be applied to folders for any type of resource.

1.3.2 Universal Discovery Probe

UCMDB relies on UD to provide deep visibility into the IT infrastructure. UD discovers CIs from various integrated data sources, passive discovery probes, agent-based, and agent-less discovery mechanism. To discover different types of CIs, UD requires a 'Discovery Activity' for that type of CI to be defined. A Discovery Activity can be defined for anything from physical infrastructure devices to logical business services. The Discovery Activities contain the credentials required to access the entities.

Passive discovery, also known as Just-in-Time discovery, performs a continuous, shallow discovery with no noise. Administration and management of the integration is done in UD itself. The UD passive discovery probe is plugged into a data-center router/switch and captures information by being connected to SPAN (or mirror) port.

Agentless discovery is the least intrusive discovery method as there is no need to deploy or maintain an agent on each server, nor is there a need to maintain a presence on discovered devices. Agentless discovery makes use of widely used industry standard software and protocols to discover new devices by connecting to various daemons and agents already present on most devices. Agentless discovery occurs using the following protocols: HTTP[10], Telnet, PowerShell, UDDI[11], VMware VIM[12] discoveries, WMI[13], NTCMD, SNMP[14], LDAP, SQL[15], JBoss, HP SIM[16], WebSphere, WebLogic, SAP[17] JMX, SAP, Siebel Gateway, UD Agent, and SSH. Only the UD Agent and SSH discovery protocols provide a secure transport mechanism using encryption.

UD then aggregates discovery results and dispatches data in bulk to UCMDB. Continuous discovery enables UCMDB to map IT hardware inventory to service dependencies, providing higher visibility and control over business services.

1.3.2.1 Universal Discovery Agent

For agent-based discovery, UD relies on the UD Agent, which is a lightweight application installed directly on the remote server. Agent-based discovery can provide visibility to remote servers behind a firewall without compromising the security of the remote network. In addition, by being present on the remote server, the UD Agent provides a more detailed view into the CI's configuration details. The UD Agent can

[10] HTTP – HyperText Transfer Protocol
[11] UDDI – Universal Description, Discovery and Integration
[12] VIM – Virtual Infrastructure Methodology
[13] WMI – Windows Management Instrumentation
[14] SNMP – Simple Network Management Protocol
[15] SQL – Structured Query Language
[16] HP SIM – Hewlett-Packard Systems Insight Manager
[17] SAP – Systems, Applications, and Products in Data Processing

also initiate data reporting when a configuration change occurs, opposed to agent-less discovery, which relies on a polling schedule.

Figure 1 below shows a UD deployment and how it is capable of discovering data from various sources.

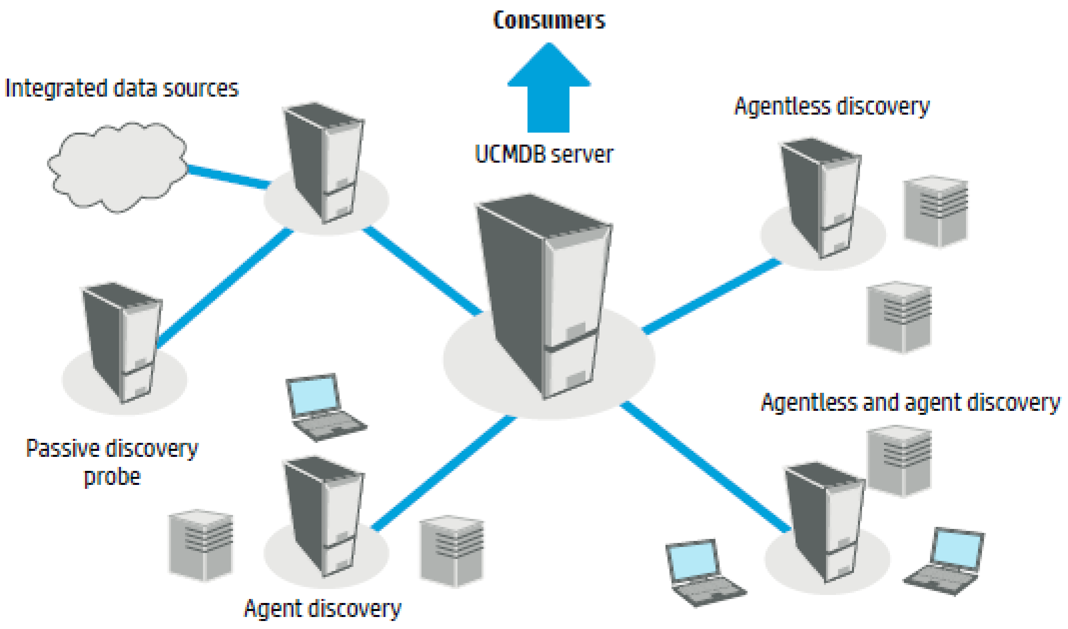

Figure 1 UD Deployment

UD supports a vast array of infrastructure and service types: high-level applications, custom or legacy applications, database components, servers and server resources, network devices, storage elements, virtualization solutions, PCs and laptops, printers, mainframes, and private/public cloud components. UD also integrates with several third-party products to support mapping of physical assets such as racks, cabling, etc. as well as deep CIs surrounding specific IT domains such as storage, server and network environments. These integrations include HP Storage Essentials, Network Node Manager, and VMware VirtualCenter (vCenter).

1.3.3 Configuration Manager

CM extends UCMDB's functionality by providing configuration managers the ability to perform policy creation, management and real-time application to all CIs added to the UCMDB. CM supports baseline hardware policies and topology policies, including policies for cluster resiliency and data quality. When a CI is detected to be in breach of a baseline hardware policy (e.g., the minimum amount of storage on a node is below a configured threshold) or a topology policy (e.g., a high availability deployment was not detected for a critical business service), configuration managers can be notified of all affected CIs in order to take action or notify the appropriate stakeholder that action is needed.

Additionally, CM provides change tracking and control over how changes are managed and communicated to the CMS consumers. CM enables data control in the CMS by maintaining the following two different 'states' for CIs:

- The 'actual state' is the service topology and configuration for the CI as it is currently being reported by the data sources of the CMS (for example, the Discovery probe).
- The 'authorized state' is a controlled state of the service topology which indicates the correct configuration of the CI according to its configuration manager.

CM imports requests for changes (RFCs) from UCMDB that were initiated in Service Manager (SM). Every RFC is associated with at least one CI and a list of applicable RFCs can be seen when viewing a CI's details. RFCs should be reviewed if a breach is detected to determine if an RFC caused a CI to violate a policy. CM's use of policies allow configuration managers to monitor undesired changes, control change against configuration standards, and report on configuration drift and policy breaches.

1.3.4 UCMDB Browser

The UCMDB Browser is a lightweight user interface (UI) that provides easy access to CI information for non-administrative users through a powerful search function as well as allows users to view the properties of CIs and their related CIs. The UCMDB Browser uses the UCMDB software development kit (SDK) application programming interface (API) to communicate with the UCMDB server. The UCMDB SDK API exposes the functionality of the UCMDB server at the individual command level. Using the downloadable UCMDB API client (retrievable from the UCMDB UI) and the UCMDB API client documentation, the UCMDB server's functionality can invoked programmatically. The UCMDB Browser allows for CIs to be searched using intuitive natural language queries. For a CI that is found as a result of a search query, relevant data is presented and gathered into information widgets (for example, the Policies widget). CI data is presented by default at a high level ('Preview mode'), but allows users the ability to delve into low level details ('Expanded mode').

Policy information from CM is displayed using the Policies widget in the UCMDB Browser. This widget is provided out of the box, and during installation the required federation configuration from Configuration Manager is created. In addition to providing visibility into CM, the UCMDB Browser can integrate with other HP software (Operations Orchestration, EnterpriseView, Application Lifecycle Management, SM, and Business Service Management) and provides a widget for each component accessible through the UCMDB Browser.

1.4 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 identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a federated CMS that discovers and collects data from physical and logical entities and services in the IT network. To discover the physical and logical network entities, the TOE uses Discovery Activities. Each Discovery Activity contains a discovery schedule and the required credentials to access the network entities. The TOE encrypts the credentials for network entities using an AES-192-bit key prior to storage in the Oracle 11g database.

Collected data is stored and analyzed upon reception by the TOE, allowing TOE administrators to perform impact analysis on proposed configuration changes, policy management and enforcement, and change tracking and control. Each physical or logical entities discovered and collected by the TOE is referred to as a CI. The TOE maintains baseline profiles for CIs, known as CITs. If a CI is detected to be different than the configuration specified in the CIT, TOE administrators may notify the CI's stakeholders, asking whether a change is required to address the discrepancy. In addition to comparing the CIs with the expected configuration according to a CIT, the TOE is able to compare the CI against TOE administrator configured policies. These policies can be related to the physical resources, configuration, or deployment needs of the CI.

The TOE provides management capabilities through the UCMDB user interface (UI), a JMX[18] interface to the UCMDB server, the exposed SDK API of the UCMDB server, the CM UI, a JMX interface to CM, and

[18] JMX – Java Management Extensions

a JMX interface to the UD Probe. The management capabilities available over the UCMDB SDK API are identical to the management capabilities available over the UCMDB UI. In addition to the management capabilities, the TOE provides non administrative users the ability to quickly query and review the collected CIs and configured policies from the configuration management database using the UCMDB Browser tool.

Audit capabilities of the TOE include the ability to audit administrative actions such as logins and logouts, TOE operator account management activities, policy creation and manipulation, and other configuration changes performed on the UCMDB (both for the UI and for JMX commands) and CM. The TOE audits all queries executed on behalf of TOE users using the UCMDB Browser. Audit logs may be viewed using the TOE's JMX interface to the UCMDB Server component.

The TOE uses a FIPS 140-2 validated cryptographic module to provide secure communication channels and paths. The TOE provides a secure connection for TOE administrative and user sessions for the UCMDB UI, UCMDB SDK APIs, UCMDB JMX interface, UCMDB Browser, CM UI, and CM JMX Interface using HTTPS[19] (via TLS). For collection and discovery operations, the TOE communicates using SSH to remote entities in the IT network. Communications between TOE components are protected using mutually-authenticated TLS sessions.

Identification and authentication is required for all TOE operators over the TOE's external interfaces prior to accessing any TSF data or functionality except the ability to query the status of the TOE, view the UCMDB class model, perform an API connection test, download the UCMDB API client (.jar file), and download the corresponding API client documentation. Any other services will require the TOE operator to authenticate. At the login screen, the TOE displays an administrator configurable warning message against unauthorized use. TOE operators may authenticate using a password credential that is obscured during entry.

Upon successful authentication, the TOE assigns the TOE operator one of five predefined roles: DataConsumer, Discovery and Integrations Admin, SuperAdmin, Viewer/TenantViewer[20], and Admin/TenantAdmin. If an authenticated session has gone idle, the TOE has the ability to terminate inactive sessions.

1.4.1 TOE Environment

The TOE is intended to be deployed in a physically secure cabinet room or data center with an appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

The Windows Server 2008 R2 underlying operating system (OS), Windows 7 OS, or RHEL[21] v5.9 OS for each TOE component and the corresponding hardware are parts of the TOE environment. The management workstation is considered part of the TOE environment as well. The TOE actively monitors the IT network for new CIs to be added to the configuration management database. The TOE requires an external authentication server for LDAP (Microsoft Active Directory) and an external exchange server (Microsoft Exchange server 2012) to be present in the TOE Environment for the CC Evaluated Configuration.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

[19] HTTPS – Hypertext Transfer Protocol – Secure

[20] TenantViewer and TenantAdmin – The prefix 'Tenant' will be added to the role name if the TOE has been configured for multi-tenancy (see section 1.3.1). Otherwise, 'Viewer' or 'Admin' will be the available role name.

[21] RHEL – Red Hat Enterprise Linux

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE boundary consists of only the UCMDB Server, UCMDB Browser, UD, and CM software. The UCMDB Server software includes the UCMDB API client that can be downloaded as one of the services the TOE provides. The TOE components are installed on RHEL v5.9 running on hardware (UCMDB Server only), the Windows Server 2008 R2 64-bit OS (UCMDB Browser, CM, and UD Probe) running on hardware, and the Windows 7 64-bit OS (UD Agent only) running on hardware. The software version for the UCMDB Server, CM, and UD components are all 10.21. The software version for the UCMDB Browser is 4.02. The deployment configuration of the TOE is shown as depicted in Figure 2 below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Hardware running Windows 2008 for the TOE (UCMDB Browser, UD Probe, and CM)
- Hardware running Windows 7 for the TOE (UD Agent only)
- Hardware running RHEL 5.9 for the TOE (UCMDB Server only)
- Each component, except UCMDB Browser needs the Java Runtime Environment (JRE) version 8 installed
- UCMDB Browser should have only Java JDK 6 or 7 for Win 64 installed, not JRE 8. Any later version of JDK must be removed from this component.
- Management workstation used to connect to the TOE, installed with:
    - Internet Explorer 8, 9, or 10
- Authentication Server to support LDAP
- Oracle 11g Database Server
- Simple Mail Transfer Protocol (SMTP) Server
- Attached IT network containing the entities to be discovered and collected into the configuration management database.

Figure 2 below shows all the TOE components (UCMDB, UD Probe, UD Agent, CM, and UCMDB Browser) in the CC Evaluated Configuration. Figure 2 contains the following undefined acronyms:

- LDAP – Lightweight Directory Access Protocol

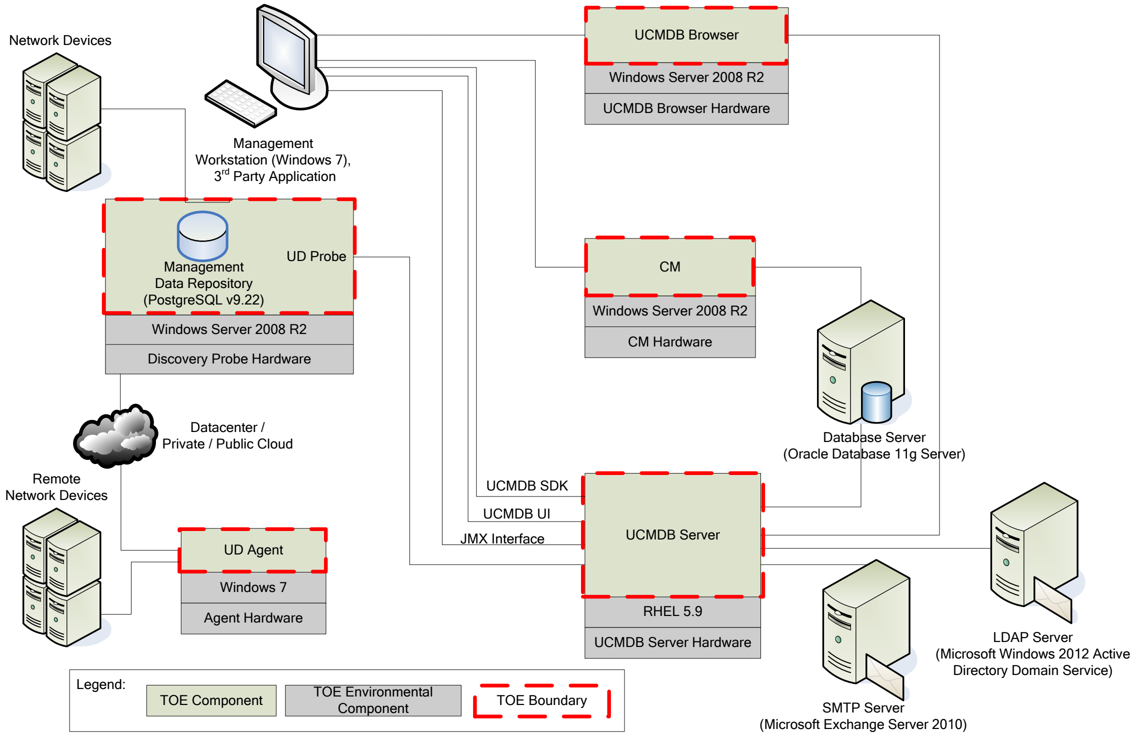
Network Devices
Management Workstation (Windows 7), 3rd Party Application
UCMDB Browser
Windows Server 2008 R2
UCMDB Browser Hardware
Management Data Repository (PostgreSQL v9.22)
UD Probe
Windows Server 2008 R2
Discovery Probe Hardware
CM
Windows Server 2008 R2
CM Hardware
Database Server (Oracle Database 11g Server)
Datacenter / Private / Public Cloud
Remote Network Devices
UCMDB SDK
UCMDB UI
JMX Interface
UCMDB Server
RHEL 5.9
UCMDB Server Hardware
UD Agent
Windows 7
Agent Hardware
LDAP Server (Microsoft Windows 2012 Active Directory Domain Service)
SMTP Server (Microsoft Exchange Server 2010)
Legend:
TOE Component
TOE Environmental Component
TOE Boundary

Figure 2 Physical TOE Boundary and CC Evaluated Configuration

1.5.1.1 Guidance Documentation

Table 2 lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

Table 2 Guidance Documentation

Document Name	Description
HP Universal CMDB, Software Version 10.21, Administration Guide, Document Release Date: July 2015, Software Release Date: July 2015	Contains detailed steps for how to properly configure and maintain the TOE.
HP Universal CMDB, Software Version 10.21, Developer Reference Guide, Document Release Date: July 2015, Software Release Date: July 2015	
HP Universal CMDB, Software Version 10.21, JMX Reference Guide, Document Release Date: July 2015, Software Release Date: July 2015	

Document Name	Description
HP Universal CMDB and Configuration Manager, Software Version 10.21, Hardening Guide, Document Release Date: July 2015, Software Release Date: July 2015	Contains a list of steps that can be performed to increase the security practices employed by the TOE.
HP Universal CMDB Configuration Manager, Software Version 10.21, User Guide, Document Release Date: July 2015, Software Release Date: July 2015	Contains a detailed description of all TOE services for the daily user of the TOE.
HP Universal CMDB, Software Version 10.21, HP UCMDB 10.21 Release Notes, Document Release Date: July 2015, Software Release Date: July 2015	Provides an overview of the changes made to HP UCMDB and UD software.
HP Universal CMDB, Software Version 10.21, Support Matrix, Document Release Date: July 2015, Software Release Date: July 2015	Provides an overview of TOE software and its hardware compatibility matrix.
Hewlett Packard Enterprise Development LP HP Universal CMDB and Universal Discovery v10.21 Guidance Documentation Supplement v0.1	Contains information regarding specific configuration for the TOE evaluated configuration.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. 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 Function Classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path/channels
- Universal Discovery and Configuration Management

1.5.2.1 Security Audit

The TOE generates log files to record auditable events. The TOE audits startup and shutdown of the audit log, login and logout events, and TOE operator account administration. The audit logs contain the identity of the user (if applicable) that an event to occur. The TOE provides TOE administrators with the ability to review the audit logs via the UCMDB JMX interface.

1.5.2.2 Cryptographic Support

The TOE utilizes the FIPS 140-2 validated RSA BSAFE Crypto-J JSAFE and JCE Software Module, Software Version 6.1 library and the OpenSSL FIPS Object Module, Software Version 2.0.7 for performing all cryptographic operations. The TOE provides cryptographic functions to secure sessions between:

- The management workstation and the TOE using TLS (for CM UI, UCMDB UI, UCMDB SDK API calls, UCMDB JMX, CM JMX, and UCMDB Browser sessions)
- TOE-to-TOE communications: UCMDB Server to UCMDB Browser, CM to UCMDB Server, UD Probe to UCMDB Server, and UD Probe to UD Agent using mutually authenticated TLS sessions

- The TOE to network entities during discovering and monitoring using SSH

Cryptographic keys are generated using a NIST[22] Special Publication (SP) 800-90A deterministic random bit generator (DRBG). Keys are securely erased when no longer needed by the application.

1.5.2.3 Identification and Authentication

The TOE enforces identification and authentication on all service requests of the TOE except for requests for UCMDB server status, API client download, and API reference documentation download. All other services require identification and authentication prior to allowing access to any TOE functionality. The TOE maintains the following list of attributes for each user: a username, a password, Role, and Tenant. When configured, the TOE supports a local password-based authentication and also remote authentication via LDAP. The LDAP server validates the username. Upon successful identification and authentication, the user is permanently associated with these attributes during the active session. The TOE also provides obscured authentication feedback during login over the UCMDB UI, UCMDB JMX interface, UCMDB Browser, and the CM UI.

1.5.2.4 Security Management

The TOE supports five default roles: DataConsumer, Discovery and Integrations Admin, SuperAdmin, Viewer/TenantViewer, and Admin/TenantAdmin. The Discovery and Integrations Admin and SuperAdmin roles have read and write access and can manage the TOE's configuration. The remaining roles, the Viewer and DataConsumer roles provide access to the collected CI information stored in the configuration management database. These roles do not provide access to configure the TSF. The management of TSF data is categorized by role and operations that can be performed for a given role. The TOE offers user management functionality that is restricted to the SuperAdmin role.

1.5.2.5 Protection the TSF

The TOE secures communications between all TOE components via mutually authenticated TLS sessions using RSA BSAFE Crypto J and the OpenSSL FIPS Object Module libraries.

1.5.2.6 TOE Access

TOE sessions that are inactive for a TOE administrator configured interval will be automatically terminated.

1.5.2.7 Trusted Paths/Channels

The cryptographic functionality of the TOE provides the TOE with the ability to create trusted paths and trusted channels. The TOE implements a trusted channel via SSH during CI discovery and collection activities. The TOE provides trusted paths between TOE operators and the UCMDB UI, UCMDB JMX Interface, UCMDB Browser, CM JMX Interface, and the CM UI via HTTPS/TLS.

The management communication path and trusted channels are distinct from other communication paths and channels and provide mutual identification and authentication. In addition, the communications are protected from modification and disclosure.

1.5.2.8 Universal Discovery and Configuration Management

The TOE provides the ability to automatically discover physical and logical entities, services, and relationships within the network (CIs) and collect information about each CI. The collected CIs are checked for compliance against policies and the corresponding CIT (the baseline expected configuration). Policies can be imported or created by a TOE administrator with the appropriate permissions and will be enforced on the CIs. If a CI is found to be in breach of a configured policy or the expected configuration according to its CIT, the TOE will generate an alert. Additionally, in multi-tenancy environments, the TOE

[22] NIST – National Institute of Standards and Technology

provides separation amongst the resources and restricts viewing of this data based on the TOE operators associated ‘Tenant’ attribute.

1.5.3 Product Physical and Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Discovery Activities over all plaintext protocols (HTTP[23], Telnet, PowerShell, UDDI[24], VMware VIM[25] discoveries, WMI[26], NTCMD, SNMP[27], LDAP, SQL[28], JBoss, HP SIM[29], WebSphere, WebLogic, SAP[30] JMX, SAP, and Siebel Gateway)
- Method invocation via the CMDB Web Service API, Data Flow Management Java API, and Data Flow Management Web Service API
- HP RUM on IT environmental components

[23] HTTP – HyperText Transfer Protocol
[24] UDDI – Universal Description, Discovery and Integration
[25] VIM – Virtual Infrastructure Methodology
[26] WMI – Windows Management Instrumentation
[27] SNMP – Simple Network Management Protocol
[28] SQL – Structured Query Language
[29] HP SIM – Hewlett-Packard Systems Insight Manager
[30] SAP – Systems, Applications, and Products in Data Processing

2 Conformance Claims

This section and Table 3 provide 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. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM as of 2014/09/05 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[31] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: 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.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 Threats

Name	Description
T.COMINT	An unauthorised person may attempt to compromise the integrity of the data discovered and events produced by the TOE by bypassing a security mechanism.
T.NOAUDIT	Threat agents may perform security-relevant operations on the TOE without being held accountable for it.
T.TRANSMIT	A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit.
T.UNAUTH	An unauthorized user may bypass the TOE server's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.
T.UNDETECT	A TOE resource may be compromised as a result of an authorized administrator not being aware a device has now become non-compliant, limiting their ability to identify and take action against a possible security problem in the TOE environment.

[31] IT – Information Technology

3.2 Organizational Security Policies

There are no Organizational Security Policies for this evaluation.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.LOCATE	The TOE is located within a controlled access facility.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMPS	The TOE environment will provide the TOE with the necessary reliable timestamps.
A.TRUSTNET	The TOE environment will include a trusted network that is protected from external interference and tampering.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 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

The specific security objectives for the TOE are listed in Table 6 below.

Table 6 Security Objectives for the TOE

Name	Description
O.ATTRIB	The TOE will be capable of maintaining user security attributes.
O.AUDIT	The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review and sort the audit trail.
O.AUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data that require authentication.
O.CRYPTO	The TOE must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.
O.DISCOVERY	The TOE must provide the ability to discover CIs and relationships in the IT network, store the discovered data, and compare the discovered Cis against configured policies and CITs. If a CI is found to be in breach of a configured policy or expected configuration according to the corresponding CIT, the TOE must provide a way to notify an administrator of the potential security violation. In multi-tenancy environments, the TOE shall restrict the viewing of Cis belonging to one tenant to only TOE operators that have the same Tenant attribute.
O.MANAGE	The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the security attributes as discussed in FMT_MSA.1, and restrict these functions and facilities from unauthorized use.
O.SECURE	The TOE shall securely transfer data with other trusted IT entities and remote users and administrators.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 IT Security Objectives

Name	Description
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.
OE.TIMESTAMPS	The operational environment will provide reliable time stamps.

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 Non-IT Security Objectives

Name	Description
NOE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
NOE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE

Table 9 Extended TOE Security Functional Requirements

Name	Description
EXT_UDC_CID	Configuration Item Discovery
EXT_UDC_PCC	Policy Creation and Compliance
EXT_ UDC_PCA	Policy Compliance Alerting
EXT_ UDC_RDR	Restricted Data Review

5.1.1 Class UDC: Universal Discovery and Configuration Management

The Universal Discovery and Configuration Management functions involve discovering physical and logical IT entities and storing and analyzing the CI. The CI's configuration is then evaluated against existing policies for compliance. Any entities found to be out of compliance will trigger an alert, which can be seen in the CM UI or be configured to send an email to the CI stakeholders. Additionally, the ability to review discovered CIs and their corresponding data is restricted to only operators with the appropriate permissions. The EXT_UDC: Universal Discovery and Collection functionality class was modeled after the CC FAU: Security audit class. The extended family EXT_UDC_CID: Configuration Item Discovery and related components were modeled after the family FAU_GEN: Audit Data Generation. The extended family and related components for EXT_UDC_PCC: Policy Creation and Compliance were modeled after the family FAU_SAA: Security Audit Analysis. The extended family EXT_UDC_PCA: Policy Compliance Alerting and related components were modeled after the CC family FAU_ARP: Security Alarms. The extended family EXT_UDC_RDR: Restricted Data Review and related components were modeled after the CC family FAU_SAR: Security Audit Review.

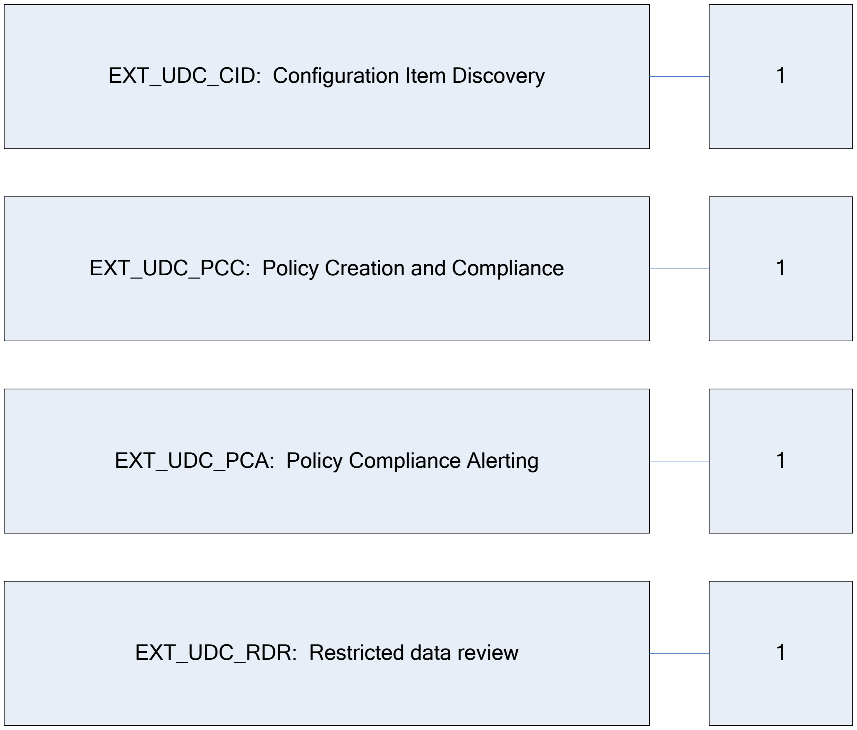
EXT_UDC_CID: Configuration Item Discovery
1
EXT_UDC_PCC: Policy Creation and Compliance
1
EXT_UDC_PCA: Policy Compliance Alerting
1
EXT_UDC_RDR: Restricted data review
1

Figure 3 EXT_UDC: Universal Discovery and Configuration Management Class Decomposition

5.1.1.1 Configuration item Discovery (EXT_UDC_CID)

Family Behaviour

This family defines the requirements for recording the occurrence of events that take place under TSF control. This family identifies the level of monitored resource data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of event-related information that should be provided within various record types.

Component Leveling

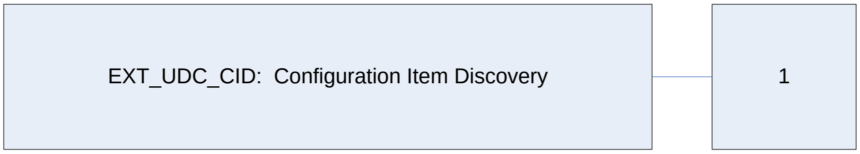

Figure 4 EXT_UDC_CID Configuration Item Discovery Family Decomposition

EXT_UDC_CID.1: Monitored resource data collection, defines the level of events and specifies the list of data that shall be captured in each event recorded.

Management: EXT_UDC_CID.1

- There are no management activities foreseen.

Audit: EXT_UDC_CID.1

- There are no auditable events foreseen.

EXT_UDC_CID.1 **Configuration Item Discovery**
Hierarchical to: **No other components**
Dependencies: **FPT_STM.1 Reliable time stamps**

EXT_UDC_CID.1.1

The TSF shall be able to perform configuration item discovery and collection of physical and logical network entities at [assignment: *specifically defined events*].

EXT_UDC_CID.1.2

At a minimum, the TSF shall collect and record the following information:

a) CI configuration data, UCMDB_ID[32], date and time of the creation of the CI, and CIT.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other CI relevant information*]

[32] ID - Identification

5.1.1.2 Policy Creation and Compliance (EXT_UDC_PCC)

Family Behaviour

This family defines the requirements for the TOE to allow for policy creation and enforcement to detect compliances breaches and potential security vulnerabilities in the collected CIs.

Component Leveling

EXT_UDC_PCC: Policy Creation and Compliance
1

Figure 5 EXT_UDC_PCC Policy Creation and Compliance Family Decomposition

EXT_UDC_PCC.1 Policy Creation and Compliance, the TSF shall provide TOE administrators the ability to configure policies that will be enforced on the collected CIs.

Management: EXT_UDC_PCC.1

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

- Management (addition, removal, or modification) of policy.

Audit: EXT_UDC_PCC.1

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

- Minimal: Record of the policy creation, modification, or deletion.

EXT_UDC_PCC.1 Policy Creation and Compliance
Hierarchical to: No other components
Dependencies: No other components

EXT_UDC_PCC.1.1

The TSF shall be able to apply a set of rules on the discovered CIs, and based upon these rules, indicate a potential security violation in the TOE environment.

EXT_UDC_PCC.1.2

The TSF shall enforce TOE administrator defined policies and CIT configuration settings against the discovered CIs.

5.1.1.3 Policy Compliance Alerting (EXT_UDC_PCA)

Family Behaviour

This family defines requirements for that the TOE that it should be able to take action if a discovered CI is found to have breached a policy or expected configuration according to its CIT. The actions to be taken based on detection of a breach can be specified using the EXT_UDC_PCA: Policy Compliance Alerting.

Component Leveling

Figure 6 EXT_UDC_PCA Policy Compliance Alerting Family Decomposition

EXT_UDC_PCA.1 Policy Compliance Alerting, specifies that the TOE will be able to provide a notification to a TOE administrator for this violation.

Management: EXT_ UDC_PCA.1
The following actions could be considered for the management functions in FMT:

- Configuration of the email address to send notifications.

Audit: EXT_ UDC_PCA.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: record of the email recipient configuration change.

EXT_UDC_PCA.1	**Policy Compliance Alerting**
Hierarchical to:	**No other components**
Dependencies:	**EXT_UDC_CID.1**

EXT_UDC_PCA.1.1

The TSF shall be able to [assignment: *list of actions*] upon the detection of a potential security problem in the TOE environment.

5.1.1.4 Restricted Data Review (EXT_UDC_RDR)

Family Behaviour

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

Component Leveling

EXT_UDC_RDR: Restricted data review
1

Figure 7 EXT_UDC_RDR Restricted Data Review family decomposition

EXT_UDC_RDR.1 Restricted data review, the TSF shall ensure that no other users other than those identified can read the CIs.

Management: EXT_UDC_RDR.1

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

- Maintenance (deletion, modification, addition) of the group of users with read access right to the CI data

Audit: EXT_UDC_RDR.1

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

- Minimal: all attempts to view CI data

EXT_UDC_RDR.1 Restricted data review

Hierarchical to: No other components

Dependencies: No dependencies

EXT_UDC_RDR.1.1

The TSF shall provide [assignment: *authorized users*] with the capability to access the CIs.

EXT_UDC_RDR.1.2

The TSF shall provide the CIs in a manner suitable for the operator to interpret the information.

EXT_UDC_RDR.1.3

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

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

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 [underlined text within brackets].
- 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 letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.1	Timing of authentication				
FIA_UAU.5	Multiple authentication mechanism		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.1	Timing of Identification		✓		
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		

Name	Description	S	A	R	I
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FTA_SSL.3	TSF-Initiated termination		✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		
EXT_UDC_CID.1	Configuration item discovery		✓		
EXT_UDC_PCC.1	Policy creation and compliance				
EXT_UDC_PCA.1	Policy compliance alerting		✓		
EXT_UDC_RDR.1	Restricted data review		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 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) [*Login and logout events and user account management*].

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 additional information*].

FAU_GEN.2 User Identity Association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FPT_STM.1 Reliable time stamps

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 [*SuperAdmin*] with the capability to read [*all audit information through the JMX interface*] 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.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm – see* Table 11 *below*] and specified cryptographic key sizes [*cryptographic key sizes – see* Table 11 *below*] that meet the following: [*list of standards* – see *Table 11* below].

Table 11 Cryptographic Key Generation Standards

Key Generation Algorithm	Key Sizes Tested	Standards (Certificate #)	
		RSA BSAFE Crypto-J	**OpenSSL FIPS Object Module v2.0.7**
HMAC[33] DRBG	HMAC-SHA[34]-256	NIST SP[35] 800-90A (CAVP[36] cert #273)	NIST SP 800-90A (CAVP cert #264)
RSA	2048, 3072	ANSI[37] X9.31 PKCS[38] #1 V1.5, RSASSA-PSS (CAVP cert #1154)	ANSI X9.31 PKCS #1 V1.5, RSASSA-PSS (CAVP cert #1145)
DSA[39]	2048, 3072	FIPS 186-4, CAVP cert #701	FIPS 186-4, CAVP cert #693
DH[40]	DH & MQV with public keys ≥ 2048 bits and private keys ≥ 224 bits	SP 800-56A, Allowed	N/A

[33] HMAC – Hash-Based Message Authentication Code
[34] SHA – Secure Hash Algorithm
[35] SP – Special Publication
[36] CAVP – Cryptographic Algorithm Validation Program
[37] ANSI – American National Standards Institute
[38] PKCS – Public Key Cryptography Standard
[39] DSA – Digital Signature Algorithm
[40] DH – Diffie Hellman

Key Generation Algorithm	Key Sizes Tested	Standards (Certificate #)	
		RSA BSAFE Crypto-J	OpenSSL FIPS Object Module v2.0.7
ECC[41] (for use in ECDH[42] and ECDSA[43])	Curves: P-224 P-256 P-384 P-521 K-224 K-256 K-384 K-521 B-224 B-256 B-384 B-521	SP 800-56A, ECDH – Allowed FIPS 186-3, ECDSA – CAVP cert #357	N/A FIPS 186-3, ECDSA – CAVP cert #347

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations – see Table 12 below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm* – see *Table 12* below] and cryptographic key sizes [*cryptographic key sizes* – see *Table 12* below] that meet the following: [*list of standards* – see *Table 12* below].

[41] ECC – Elliptic Curve Cryptography
[42] ECDH – Elliptic Curve Diffie Hellman
[43] ECDSA – Elliptic Curve Digital Signature Algorithm

Table 12 Cryptographic Operation

Algorithm	Standard and Cert #	
	RSA BSAFE Crypto-J	**OpenSSL FIPS Object Module v2.0.7**
Symmetric Key Encryption/Decryption Algorithms		
AES: ECB[44], CBC[45], OFB[46], CFB[47] CTR[48], CCM[49], GCM[50], XTS[51,52,53]-128 bit mode for 128-, 192-, and 256-bit key sizes	FIPS 197, CAVP cert #2249	FIPS 197, CAVP cert #1884
Triple-DES[54]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	FIPS 46-3, CAVP cert #1408	FIPS 46-3, CAVP cert #1398
Digital Signature Generation/Verification Algorithms		
RSA X9.31, PKCS#1 V.1.5, RSASSA-PSS Signature generation; Signature verification – 1024- (signature verification only), 2048-, 3072-bit	ANSI[55] X9.31 (FIPS 186-4), CAVP cert #1154	ANSI X9.31 (FIPS 186-4), CAVP cert #1145
DSA Signature generation; Signature verification – 1024- (Signature verification only), 2048-, 3072-bit	FIPS 186-4, CAVP cert #701	FIPS 186-4, CAVP cert #693
ECDSA Signature generation for all NSA[56] Suite B P, K, and B Curves, Signature Verification for all P, K, and B curves.	FIPS 186-4, CAVP cert #357	FIPS 186-4, CAVP cert #347
Key Derivation		
KDFTLS10, KDFTLS12 with SHA-256, SHA-384, SHA-512	SP 800-135, CAVP cert #39	N/A
Hashing Functions Asymmetric Key Algorithms		
SHA-1, 224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256	FIPS 180-2, CAVP cert #1938	FIPS 180-2, CAVP cert #1923
Message Authentication Code (MAC) Functions		
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 198, CAVP cert #1378	FIPS 198, CAVP cert #1363

[44] ECB – Electronic Codebook
[45] CBC – Cipher Block Chaining
[46] OFB – Output Feedback
[47] CFB – Cipher Feedback
[48] CTR – Counter Mode
[49] CCM – Counter with CBC-MAC
[50] GCM – Galois Counter Mode
[51] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[52] XEX – XOR-Encrypt-XOR
[53] XOR – Exclusive Or
[54] DES – Data Encryption Standard
[55] ANSI – American National Standards Institute
[56] NSA – National Security Agency

6.2.3 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: [*username, password, Tenant, and role*].

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1

The TSF shall allow [

- *Query the operational status of the UCMDB Server*
- *View the UCMDB Class model*
- *Perform and API Connection Test*
- *Download the API client (.jar file)*
- *Download the corresponding API client documentation*]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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 [*the following authentication mechanisms:*

- *password-based*
- *LDAP authentication*

] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [

- *Password-based authentication is performed according to the verification of identity and credential information*
- *LDAP authentication - The username is validated against LDAP. If the validation is successful, the user is granted access assigned the stored role with the username*].

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1

The TSF shall provide only [*obscured feedback in the form of bullets*] to the user while authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1

The TSF shall allow [

- *Query the operational status of the UCMDB Server*
- *View the UCMDB class model*
- *Perform an API Connection Test*
- *Download the API client (.jar file)*
- *Download the corresponding API client documentation*]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

6.2.4 Class FMT: Security Management

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 [modify the behaviour of] the functions [

- *Session timeouts*
- *Auditing*
- *Email based notifications*
- *Authentication]*

to [*SuperAdmin*].

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 [modify] the [*general TOE configuration data, alert settings, session timeout interval, TOE operator accounts, policies, Discovery Activities, breach of policy alert method, audit severity level, and audit data*] to [*SuperAdmin*].

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: [*operator account management, SMTP configuration for alerts, authentication method, inactivity session timer configuration, Discovery Activity configuration, and policy creation and management]*.

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 [*DataConsumer*, *Discovery and Integrations Admin, SuperAdmin, Viewer/TenantViewer, Admin/TenantAdmin*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_ITT.1.1

The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

6.2.6 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*SuperAdmin-configurable time interval*].

6.2.7 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies

FTP_ITC.1.1

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

FTP_ITC.1.2

The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*CI discovery and collection*].

FTP_TRP.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication, [*all other services on the UCMDB UI, UCMDB SDK APIs, UCMDB JMX interface, UCMDB Browser, CM UI, and CM JMX Interface]*].

6.2.8 Class UDC: Universal Discovery and Configuration Management

EXT_UDC_CID.1 Configuration Item Discovery
Hierarchical to: No other components
Dependencies: FPT_STM.1 Reliable time stamps

EXT_UDC_CID.1.1

The TSF shall be able to perform CI discovery and collection of physical and logical network entities at [*Discovery and Integrations Admin or SuperAdmin defined time interval*].

EXT_UDC_CID.1.2

At a minimum, the TSF shall collect and record the following information:

a) CI configuration data, UCMDB_ID, date and time of the creation of the CI, and CIT.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*impact simulation information, stakeholder list (if applicable), change history, and environmental details*]

EXT_UDC_PCC.1 Policy Creation and Compliance
Hierarchical to: No other components
Dependencies: No other components

EXT_UDC_PCC.1.1

The TSF shall be able to apply a set of rules on the discovered CIs, and based upon these rules, indicate a potential security violation in the TOE environment.

EXT_UDC_PCC.1.2

The TSF shall enforce TOE administrator defined policies and CIT configuration settings against the discovered CIs.

EXT_UDC_PCA.1 Policy Compliance Alerting
Hierarchical to: No other components
Dependencies: EXT_UDC_CID.1

EXT_UDC_PCA.1.1

The TSF shall be able to [

- *Provide an email notification to the CI stakeholder*]

upon the detection of a potential security problem in the TOE environment.

EXT_UDC_RDR.1 Restricted data review
Hierarchical to: No other components
Dependencies: No dependencies

EXT_UDC_RDR.1.1

The TSF shall provide [*SuperAdmin, Admin, Discovery and Integrations Admin, and Data Consumer*] with the capability to access the CIs.

EXT_UDC_RDR.1.2

The TSF shall provide the CIs in a manner suitable for the operator to interpret the information.

EXT_UDC_RDR.1.3

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

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 13 Assurance Requirements summarizes the requirements.

Table 13 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	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
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Complete functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Focused Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 14 lists the security functions and their associated SFRs.

Table 14 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of Identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
TOE Access	FTA_SSL.3	TSF-Initiated termination
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
Universal Discovery and Configuration Management	EXT_UDC_CID.1	Configuration item discovery
	EXT_UDC_PCC.1	Policy creation and compliance
	EXT_UDC_PCA.1	Policy compliance alerting
	EXT_UDC_RDR.1	Restricted data review

7.1.1 Security Audit

The TOE is capable of auditing a variety of events, including startup and shutdown of the system, login and logout events, and TOE operator account management. For each action that is invoked by a TOE operator, the TOE will associate his or her username with the generated audit log. The TOE generates an audit event for startup and shutdown of the system, which is tied to the startup and shutdown of the audit functionality. Since the system starts up and shuts down at the same time as the audit function, these records can be considered to provide equivalent notice.

The Audit Log entries contain at a minimum the following fields:

- Date and time of the event
- Type of event
- Identity of the subject
- Outcome of the event

The TOE does not audit any additional fields in addition to these fields. The SuperAdmin role accessing the UCMDB JMX interface has the ability to review the audit logs by accessing the ‘Server Services -> showLog’ option.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1.

7.1.2 Cryptographic Support

Cryptographic operations necessary to support SSH, TLS, HTTPS, encryption, decryption, and key generation are provided by two CMVP[57] validated libraries: the RSA B-SAFE Crypto-J JSAFE and JCE Cryptographic Library v6.1 (Certificate #2057) and the OpenSSL FIPS Object Module, Software Versionv2.0.7 (Certificate #1747). For a complete list of the cryptographic algorithms, modes, and key sizes, please see Table 12 above. The TOE uses HTTPS via TLS to protect administrative communications over the UCMDB UI, UCMDB JMX interface, UCMDB SDK API calls, CM UI, CM JMX, and UCMDB Browser. During CI discovery and collection activities, when configured, communications are protected using the SSH protocol. For both TLS and SSH session keys, the TOE uses symmetric AES and Triple-DES keys to encrypt and decrypt data.

Keys are generated via the use of the HMAC_DRBG to provide random keying material. The TOE implements DH, DSA, RSA, and ECC (ECDSA and ECDH) key-pair establishment methods.

To secure the entity credentials that are stored in the Oracle 11g database in the TOE environment, the TOE uses an AES-192-bit key to encrypt credentials prior to storage in the database.

The TOE provides zeroization techniques that meets the FIPS 140-2 zeroization requirement for all plaintext secret and private keys. TLS and SSH session keys reside in volatile memory only and never stored persistently. The contents of volatile memory are lost immediately when power is removed or the TOE is restarted; therefore, TLS and SSH session keys are considered zeroized when the TOE is restarted or shutdown.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

[57] CMVP – Cryptographic Module Validation Program

7.1.3 Identification and Authentication

The TOE supports the Identification and Authentication TSF for all external interfaces. The TOE allows unauthenticated operators to query the operational status of the UCMDB server, view the UCMDB class model, perform an API connection test, download the API client (.jar file), and download the corresponding API client documentation. All other TOE functionality requires that TOE operators authenticate using a password. For all TOE operators, the TOE maintains username, password, role, and Tenant attributes. All attributes can be modified by the SuperAdmin over the UCMDB UI or JMX interface.

The TOE can be configured to use a local password based authentication mechanism or remotely via LDAP authentication. If a TOE operator is authenticating using a password based credential, the TOE obscures feedback during password entry in the form of bullets ('•') over the UCMDB UI, UCMDB JMX interface, UCMDB Browser, UD JMX interface, CM UI and CM JMX interface.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1.

7.1.4 Security Management

The TOE provides management facilities to TOE operators for TSF data and security functions. TSF data includes general TOE configuration data, Discovery Activity, operator accounts, authentication mechanism, policy creation, and auditing. The TOE maintains roles that provide varying levels of privileges that determine what TSF data an authenticated operator can access. Table 15 below lists the roles supported by the TOE.

Table 15 TOE Roles

Role Name	Description
DataConsumer	The role has read-only permission for resources and CIs and access to the UCMDB UI and the Reports module only.
Discovery and Integrations Admin	Full permission for all Data Flow Management (Discovery configuration) without tenant assignment permissions. Includes permissions for all actions that are required to perform any discovery-related flows. It also includes permission for discovery-related tasks such as managing probes, credentials, and adapters and for viewing discovery-related reports.
SuperAdmin	Full read/write permissions for all TOE functionality.
Viewer/TenantViewer	Viewer – Read only permission for resources and CIs and access to all Modeling modules except for Enrichment Manager, without tenant assignment permission (only relevant when multi-tenancy is not enabled). TenantViewer – Read only permission for resources and CIs and access to all Modeling modules except for Enrichment Manager. Also includes read only permission for tenant assignment (only relevant when multi-tenancy is enabled).

Role Name	Description
Admin/TenantAdmin	Admin – Full permission for resources and CIs and access to all Modeling modules except for Enrichment Manager, without tenant assignment permission (only relevant when multi-tenancy is not enabled). Also includes all permissions associated with HP Universal CMDB Configuration Manager. TenantAdmin – Full permission for resources and CIs and access to all Modeling modules.

TOE operator accounts can be managed via the UCMDB UI under the **Security -> Roles Manager** menu option. Only the SuperAdmin role can use this facility to modify operator attributes, (username, password, Tenant, role), create, and delete operators.

The TOE provides the SuperAdmin role the capability to manage the authentication mechanisms used by the TOE. The SuperAdmin may configure the TOE to use password-based or LDAP authentication.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE provides protection of TSF data from disclosure and modification while in transit between different parts of the TOE. The TOE secures the following communication channels using mutually authenticated TLS sessions:

- UCMDB Server and the UCMDB Browser
- UCMDB Server and CM
- UCMDB Server and UD Probe
- UD Probe and UD Agent

TOE Security Functional Requirements Satisfied: FPT_ITT.1.

7.1.6 TOE Access

The TOE actively monitors authenticated sessions for inactivity and is capable of terminating sessions after a SuperAdmin-configurable time period of inactivity.

TOE Security Functional Requirements Satisfied: FTA_SSL.3.

7.1.7 Trusted Path/Channels

The TOE provides a trusted path between the TOE management interfaces and remote TOE operators. The remote interfaces that are secured include the UCMDB UI (HTTPS via TLS), UCMDB SDK API calls (HTTPS via TLS), UCMDB JMX interface (HTTPS via TLS), UCMDB Browser (HTTPS via TLS), CM UI (HTTPS via TLS), and the CM JMX interface (HTTPS via TLS). The protocols and the cryptography implemented by the TOE protect communications against unauthorized disclosure and modification of TSF data while it is in transit. The UD JMX interface does not support a trusted path for management and therefore should only be accessed from the trusted network within the secured access facility in the evaluated configuration.

Additionally, the TOE provides a trusted channel between the TOE and trusted IT entities. Trusted IT entities consist of the network entity CIs. The trusted channel used to secure the communications between the network entities and the TOE is provided via SSH to prevent unauthorized disclosure and modification of the remote entity credentials and the CI configuration details that are collected.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1.

7.1.8 Universal Discovery and Configuration Management

The TOE is capable of automatically discovering and managing business service definitions, management data repositories, IT infrastructure relationships, and detailed asset information. The TOE performs discovery through the UD Probe and UD Agent components according to configured 'Discovery Activities.' Each 'Discovery Activity' has an associated execution schedule detailing the start, stop, and repeated interval times for discovery. Each CI discovered will be stored with the time that it was discovered, a UCMDB_ID reference, the configuration data specific to the CI, and the CIT. The TOE restricts the ability to view the collected CIs to only authorized TOE operators who have been granted permission. Permission can be granted through role assignment or on an individual CI basis. Permission to view CIs can be explicitly granted or revoked to and from any existing role by the SuperAdmin.

TOE administrators may craft policies to be applied to the collected CIs to determine if they are operating in compliance with the policy. In addition to comparing the CIs to the policies, the CIs can also be compared to the corresponding CIT to determine if there are any unexpected configuration settings according to the CIT. If a CI is found to be out of compliance with a policy, the TOE provides alerting capabilities by sending an email to a TOE administrator defined email address.

The TOE has the ability to automatically discover physical and logical entities, services, and relationships (collectively referred to as CIs) within the network and collect information about each CI. The collected CIs are checked for compliance against policies and the corresponding CIT (the baseline expected configuration). Policies can be imported or created by a TOE administrator with the appropriate permissions and will be enforced on the CIs. If a CI is found to be in breach of a configured policy or the expected configuration according to its CIT, the TOE will generate an alert. Additionally, in multi-tenancy environments, the TOE provides separation amongst the resources and restricts viewing of this data based on the TOE operators associated 'Tenant' attribute.

TOE Security Functional Requirements Satisfied: EXT_UDC_DCD.1, EXT_UDC_NCE.1, EXT_UDC_PCM.1, EXT_UDC_RDR.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 below provides a mapping of the objects to the threats they counter.

Table 16 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.COMINT An unauthorised person may attempt to compromise the integrity of the data discovered and events produced by the TOE by bypassing a security mechanism.	O.AUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data that require authentication.	O.AUTH mitigates this threat by ensuring that the TOE requires identification and authentication of users prior to any TSF data access.
T.NOAUDIT Threat agents may perform security-relevant operations on the TOE without being held accountable for it.	O.AUDIT The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review and sort the audit trail.	O.AUDIT mitigates this threat by ensuring that security relevant events of the TOE are preserved through an audit trail.
T.TRANSMIT A user or process may be able to bypass the TOE's security mechanisms and gain access to the data while the data is in transit.	O.CRYPTO The TOE must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.	O.CRYPTO mitigates this threat by ensuring that the cryptographic keys are managed securely conformant to the FIPS 140-2 standards.
	O.SECURE The TOE shall securely transfer data with other trusted IT entities and remote users and administrators.	O.SECURE mitigates this threat by providing trusted mechanisms to protect the TOE data that is transferred between trusted IT entities and remote users.

Threats	Objectives	Rationale
T.UNAUTH An unauthorized user may bypass the TOE server's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.	O.ATTRIB The TOE will be capable of maintaining user security attributes.	O.ATTRIBUTES mitigates this threat by allowing only users with valid credentials to access the TOE.
	O.AUDIT The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review and sort the audit trail.	O.AUDIT mitigates this threat by ensuring that unauthorized attempts to access the TOE or TSF-mediated resources are recorded.
	O.AUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data that require authentication.	O.AUTH mitigates this threat by ensuring that users are identified and authenticated prior to gaining access to TOE server functions.
	O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the security attributes as discussed in FMT_MSA.1, and restrict these functions and facilities from unauthorized use.	O.MANAGE mitigates this threat by ensuring that access to TOE security data is limited to only authorized users with access to the management functions of the TOE server.
T.UNDETECT A TOE resource may be compromised as a result of an authorized administrator not being aware a device has now become non-compliant, limiting their ability to identify and take action against a possible security problem in the TOE environment.	O.DISCOVERY The TOE must provide the ability to discover Cis and relationships in the IT network, store the discovered data, and compare the discovered Cis against configured policies and CITs. If a CI is found to be in breach of a configured policy or expected configuration according to the corresponding CIT, the TOE must provide a way to notify an administrator of the potential security violation. In multi-tenancy environments, the TOE shall restrict the viewing of Cis belonging to one tenant to only TOE operators that have the same Tenant attribute.	O.AUTO mitigates this threat by ensuring that the TOE will discover and monitor devices in the network for compliance through Policy checks. If a Policy check fails, the TOE will automatically generate an event and invoke an administrator defined action to ensure that no potential security violations go undetected.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this evaluation.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 17 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM satisfies this assumption by ensuring that the TOE hardware meets minimum requirements and the OS supports all the TOE functions.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the TOE environment.	OE.PHYSICAL satisfies the assumption by ensuring that the TOE environment provides protection from unauthorized modification.
A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NO_EVIL Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	OE.NO_EVIL satisfies this assumption by ensuring that administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	OE.PROTECT satisfies the assumption by ensuring that the TOE environment provides protection from unauthorized modification.
A.TIMESTAMPS The TOE environment will provide the TOE with the necessary reliable timestamps.	OE.TIMESTAMPS The operational environment will provide reliable time stamps.	OE.TIME_STAMPS satisfies this assumption by stating that the environment will maintain reliable timestamps and those will be used by the TOE to stamp each audit record with a date and time.
A.TRUSTNET The TOE environment will include a trusted network that is protected from external interference and tampering.	OE.PROTECT The TOE environment must protect itself, the network on which the TOE is deployed, and the TOE from external interference or tampering.	The TOE environment provides protection from external interference and tampering through the use of an internal trusted network. OE.PROTECT satisfies this assumption.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A class of EXT_UDC requirements was created to specifically address the analysis of the stored asset data. The CC FAU: Security Audit class was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of asset data monitoring and provide for requirements for alerting when violations are detected. These requirement's dependencies have been noted in 5.1.1. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended Security Assurance Requirements have been defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 below shows a mapping of the objectives and the SFRs that support them.

Table 18 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ATTRIB The TOE will be capable of maintaining user security attributes.	FMT_MTD.1 Management of TSF data	The TOE is required to ensure that only authorized users are allowed access to TSF data by their assigned permissions.
	FMT_SMR.1 Security roles	The TOE is required to manage the defined user roles. The TOE does this by ensuring that only authorized users have access to TSF data.
O.AUDIT The TOE must be able to generate audit records, record the identity of the user that caused when event (when applicable), and provide authorized administrators with the ability to review and sort the audit trail.	FAU_GEN.1 Audit data generation	The TOE is required to record audit events as defined in this SFR. This requirement ensures that the administrator has the ability to audit security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event.
	FAU_GEN.2 User identity association	The TOE is required to associate auditable events with the identity

Objective	Requirements Addressing the Objective	Rationale
		of the user that caused the event.
	FAU_SAR.1 Audit review	The TOE is required to present the audit logs to the authorized administrator in a suitable manner for interpretation.
O.AUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data that require authentication.	FIA_UAU.1 Timing of authentication	The TOE is required to successfully authenticate a user before allowing access to TOE functions except those explicitly listed.
	FIA_UAU.5 Multiple authentication mechanism	The TOE is required to authenticate users requesting access to the TSF before any actions may be taken on the behalf of that user. There are multiple authentication mechanisms supported as specified in this SFR.
	FIA_UAU.7 Protected authentication feedback	The TOE is required to obscure the feedback of passwords entered by users of the TOE during authentication.
	FIA_UID.1 Timing of Identification	The TOE is required to successfully identify a user before allowing access to TOE functions except those explicitly listed.
	FMT_MOF.1 Management of security functions behavior	The TOE is required to authenticate users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behavior of the TOE.
	FTA_SSL.3 TSF-Initiated termination	The TOE is required to protect TSF data by ensuring that unauthorised users do not gain access to the TOE through an unattended session.
O.CRYPTO The TOE must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.	FCS_CKM.1 Cryptographic key generation	The TOE is required to generate cryptographic keys in accordance with FIPS 140-2 approved techniques.
	FCS_CKM.4 Cryptographic key destruction	The TOE is required to destroy cryptographic keys according to FIPS 140-2 zeroization requirements.
	FCS_COP.1	The TOE is required to perform

Objective	Requirements Addressing the Objective	Rationale
	Cryptographic operation	cryptographic operations according to the FIPS 140-2 approved algorithms and key sizes.
O.DISCOVERY The TOE must provide the ability to discover Cis and relationships in the IT network, store the discovered data, and compare the discovered Cis against configured policies and CITs. If a CI is found to be in breach of a configured policy or expected configuration according to the corresponding CIT, the TOE must provide a way to notify an administrator of the potential security violation. In multi-tenancy environments, the TOE shall restrict the viewing of Cis belonging to one tenant to only TOE operators that have the same Tenant attribute.	EXT_UDC_CID.1 Configuration item discovery	The TOE is required to provide the ability to discover CIs in the network and collect and store the data in the configuration management database.
	EXT_UDC_PCA.1 Policy compliance alerting	Upon detection of a security breach within a discovered CI, the TOE is required to be generate an alert that notifies a TOE administrator of the potential threat in the TOE environment.
	EXT_UDC_PCC.1 Policy creation and compliance	The TOE must provide the ability for TOE administrators to define and apply a set of rules to determine if discovered and collected CIs are configured in known good state.
	EXT_UDC_RDR.1 Restricted data review	The TOE is required to restrict the viewing of Cis belonging to a specific Tenant to only TOE operators that have the same Tenant attribute specified.
O.MANAGE The TOE must provide all the functions and facilities necessary to support the authorized administrator in management of the security attributes as discussed in FMT_MSA.1, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1 Management of security functions behavior	The TOE is required to restrict administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The TOE is required to restrict access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The TOE is required to include administrative functions to facilitate the management of security attributes.
	FMT_SMR.1 Security roles	The TOE is required to associate users with roles to provide access to TSF management functions and data.
O.SECURE The TOE shall securely transfer data with other trusted IT entities and remote users and administrators.	FPT_ITT.1 Basic internal TSF data transfer protection	The TOE is required to provide a secure channel used to protect TSF data transmitted between the TOE server and TOE satellite.
	FTP_ITC.1	The TOE is required to provide a

Objective	Requirements Addressing the Objective	Rationale
	Inter-TSF trusted channel	trusted communication path between itself and an external trusted IT entity which provides for the protection of the data from disclosure and modification when in transit.
	FTP_TRP.1 Trusted path	The TOE is required to provide a trusted communication path between itself and remote users which provides for the protection of the data from disclosure and modification when in transit.

8.5.2 Security Assurance Requirements Rationale

EAL2 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 software engineering 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. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's flaw reporting procedures.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 19 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 19 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the TOE environment. An environmental objective states that the TOE will receive reliable time stamps.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2,

SFR ID	Dependencies	Dependency Met	Rationale
			which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FIA_ATD.1	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	None	N/A	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	None	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_ITT.1	None	N/A	
FTA_SSL.3	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	
EXT_UDC_CID.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the TOE environment. An environmental objective states that the TOE will receive reliable time stamps.
EXT_UDC_PCC.1	None	N/A	
EXT_UDC_PCA.1	EXT_UDC_CID.1	✓	
EXT_UDC_RDR.1	None	N/A	

9 Acronyms

Table 20 below defines the acronyms used throughout this document.

Table 20 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter Mode with CBC-MAC
CFB	Cipher Feedback
CI	Configuration Item
CIT	Configuration Item Type
CM	Configuration Management
CMS	Configuration Management System
CMVP	Cryptographic Module Validation Program
CN	Common Name
CTR	Counter Mode
DES	Data Encryption Standard
DH	Diffie Hellman
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois Counter Mode
HMAC	Hash-Based Message Authentication Code
HP	Hewlett-Packard
HTTPS	Hypertext Transfer Protocol – Secure
IT	Information Technology

Acronym	Definition
JCE	Java Cryptography Extension
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MDR	Management Data Repository
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OFB	Output Feedback
OS	Operating System
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RSA	Rivest, Shamir, and Adleman
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SHA	Secure Hash Algorithm
SFR	Security Functional Requirement
SP	Special Publication
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UCMDB and UD	Universal Configuration Management Database, Universal Discovery, and Configuration Manager with Universal Configuration Management Database Browser
UI	User Interface
UPN	User Principal Name
XEX	XOR-Encrypt-XOR
XOR	Exclusive Or
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Prepared by:
Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com