National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Unified Computing System (UCS)

Report Number: CCEVS-VR-VID10403-2011
Dated: 30 December 2011
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Kenneth B. Elliott, III (Senior Validator)

The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
Gary Grainger
Eve Pierre
Quang Trinh

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Clarification of Scope in Section 4 and the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Unified Computing System (UCS). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Cisco Unified Computing System was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in December 2011.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Reports (ETR) and the associated test report. The ST was written by Cisco Systems, Inc. The ETR and test report used in developing this validation report were written by SAIC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, dated July 2009 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R3, dated July 2009. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Cisco Unified Computing System Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 4 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE consists of hardware and software components that support Cisco's unified fabric, which run multiple types of data-center traffic over a single converged network adapter. The UCS features a role based access control policy to control the separation of administrative duties and provides a security log of all changes made.

A validation team from CCEVS monitored the activities of the evaluation team, reviewed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concluded that SAIC's findings are accurate, the conclusions justified, and the conformance

results are correct. The conclusions of SAIC in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance results of the evaluation;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2100 and 2200 Series Fabric Extenders, and 6100 Series Fabric Interconnects with UCSM 1.4(1m)
Protection Profile	N/A
Security Target	*Cisco Unified Computing System (UCS) Security Target*, Version 1.0, December, 2011
Dates of evaluation	March 2010 through December 2011
Evaluation Technical Report	*Evaluation Technical Report for the Cisco Unified Computing System (UCS) Part 1, (Non-Proprietary)*, Version 1.0, November 11, 2011 *Evaluation Technical Report for the Cisco Unified Computing System (UCS), (Proprietary)*, Version 2.0, November 11, 2011
Conformance Result	Part 2 extended conformant and EAL4 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on March 22, 2010
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July 2009 and all applicable NIAP and International Interpretations effective on March 22, 2010
Sponsor	Cisco Systems, Inc.,
Developer	Cisco Systems, Inc.,
Common Criteria Testing Lab	SAIC Inc., Columbia, MD
Evaluators	Tammy Compton, Julie Cowan, Eve Pierre, Gary Grainger and Quang Trinh of SAIC, Columbia, Maryland
Validation Team	Kenneth B. Elliott III and Mike Allen of The Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None.

International Interpretations

None.

3 Security Policy

This section summarizes the following security functionality of the TOE:

Security Audit
Identification and Authentication
Security Management
Network Separation
Role Based Access Control

3.1 Security Audit

The Unified Computing System stores audit information in three different formats: audit log, events, and faults. This information is compiled to assist the administrator in monitoring the security state of the UCS as well as trouble shooting various problems that arise throughout the operation of the system. All three types of information are stored within an SQLite database stored on the Fabric Switch. The database is internal only and does not provide any externally visible interfaces for communication. When the UCS is deployed in a clustered configuration, all instances of the UCS Manager record audit information with the primary UCS Manager instance. In standalone mode, all audit data are stored locally. Regardless of standalone or clustered configuration, the TOE may be configured to send records to an external syslog server, in which case syslog is a supplemental service for monitoring, alerting and reporting, not the audit log storage mechanism of the TOE. Audit log storage and protection functionality comes from the TOE itself.

The UCS Manager TOE component provides the ability to audit the actions taken by authorized administrators. Audited events include start-up and shutdown, configuration changes, administrative authentication, and administrative log-off.

The TOE provides the capability for authorized administrators to review the audit records stored within the TOE

3.2 Identification and Authentication

Cisco UCS supports two methods of authenticating administrator logins on the Cisco UCS Manager: a local user database of passwords (and optionally SSH keys) or a remote authentication server accessed either via LDAP, RADIUS, or TACACS+. The TOE may be configured to use either the local user database or one of the remote authentication methods, but multiple authentication methods may not be selected. Remote authentication may be used to centralize user account management to an external authentication server. When the UCS is deployed in a clustered configuration, all instances of the UCS Manager share the local user database.

The system has a default user account, admin, which cannot be modified or deleted. This account is the system administrator account and has full privileges. Each user account must have a unique user name that is not all numeric and does not start with a number. For authentication purposes, a password is required for each user account. User accounts can be configured to expire at a predefined time. When the expiration time is reached the account is locked and must be unlocked by an authorized administrator. By default, user accounts do not expire.

Identification and Authentication services are also extended to the Cisco Integrated Management Controller (CIMC) via IPMI Access Profiles. These provide the ability to access the CIMC via the Intelligent Platform Management Interface (IPMI) using a username/password database stored on the CIMC.

3.3 Security Management

UCS can be managed using the graphical user interface (over SSL3.1/TLS1.0), the command line (over SSHv2 or by local console access via the RS-232 port), or by manipulating an XML API. Each of these interfaces can be used in the evaluated configuration to administer the UCS. The interfaces all operate on the same XML data structures and provide identical functionality. For all management channels, users have a default read-only authorization to access non-sensitive management objects (keys and passwords are never exposed to an external management interface). Additional user privileges each grant access to modify specific management objects.

An administrator can use Cisco UCS Manager to perform management tasks for all physical and virtual devices within a Cisco UCS instance.

3.4 Network Separation

The TOE enforces several information flow control policies, including VLAN and VSAN separation policies. Each of these enforced information flows are further discussed below.

3.4.1 VLAN Separation

VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN.

The most important requirement of VLANs is the ability to identify the origination point for packets with a VLAN tag to ensure packets can only travel to interfaces for which they are authorized.

The Cisco UCS 6100 Series Fabric Switch Hardware requires VLANs to function. When the administrator configures network adapters on a per server basis, VLANs are specified for each adapter.

3.4.2 VSAN Separation

Virtual SAN (VSAN) technology partitions a single physical Storage Area Network (SAN) into multiple VSANs. VSAN capabilities allow the Cisco UCS 6100 Series Fabric Switch Hardware to logically divide a large physical fabric into separate isolated environments to improve SAN scalability, availability, manageability, and network security.

Each VSAN is a logically and functionally separate SAN with its own set of Fibre Channel fabric services. This partitioning of fabric services greatly reduces network instability by containing fabric reconfigurations and error conditions within an individual VSAN. The strict traffic segregation provided by VSANs helps ensure that the control and data traffic of a given VSAN is confined within its own domain, increasing SAN security.

Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between user groups. This ensures the confidentiality of data traversing the VSAN from users and devices belonging to other VSANs. It should be noted that devices, such as file servers and tape storage devices are not part of the TOE but part of the TOE environment and may be configured to participate in a VSAN. Each network interface of a device connected to the TOE may only participate in a single VSAN.

3.5 Role Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization, but would not be able to update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

3.5.1 Privileges

Privileges give their holder access to specific system resources and permission to perform specific tasks. Privileges can be added to the default roles.

The following table lists each privilege and the user role given that privilege by default.

Table 2: Privileges and Default Role Assignments

Privilege	Management Capabilities	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator

ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-	Service profile pool policy	Server Profile Administrator

policy		
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

3.5.2 User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has storage related privileges, and Role2 has server related privileges, then users who are assigned to both Role1 and Role2 have storage and server related privileges.

All roles include read access to all configurations on the system, and all roles except Read-Only can modify some portion of the system state. A user assigned a role can modify the system state in that user's assigned area.

The system contains the following default user roles:

- AAA Administrator: Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.
- Administrator: Complete read-and-write access to the entire system. The default admin account is assigned this role by default and this association cannot be changed.
- Facility Manager: Read-and-write access to power management operations.
- Network Administrator: Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system.
- Operations: Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.
- Read-Only: Read-only access to system configuration with no privileges to modify the system state.
- Server Equipment Administrator: Read-and-write access to physical server related operations. Read access to the rest of the system.
- Server Profile Administrator: Read-and-write access to logical server related operations. Read access to the rest of the system.
- Server Security Administrator: Read-and-write access to server security related operations. Read access to the rest of the system.
- Storage Administrator: Read-and-write access to storage operations. Read access to the rest of the system.

New custom roles may be created, deleted, or modified to add or remove any combination of privileges. Default roles may be deleted or modified except the ‘admin’ and ‘read-only’ roles. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you

can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts. User profiles on AAA servers (RADIUS or TACACS+) contain the roles corresponding to the privileges granted to that user. The cisco-av-pair vendor-specific attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

3.5.3 User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) to which the user is allowed access, and access is limited to the organizations specified in the locale. Access control based on locales is enforced on all roles, including the full access Administrator role. A locale without any organizations may be created, this grants unrestricted access to system resources in all organizations.

Users with AAA Administrator privileges (AAA Administrator role) or the Administrator role can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

Administrators can hierarchically manage organizations. A user that is assigned at a top-level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

4 Assumptions and Clarification of Scope

The following assumptions were made during the evaluation of Cisco Unified Computing System (UCS):

- All authorized administrators are assumed to be not evil and will not disrupt the operation of the UCS system intentionally.
- Each network interface of a device connected to the TOE may only participate in a single VSAN.
- The UCS system must be separated from the public Internet or a public network by an application aware firewall.
- The facility housing the UCS system must have a physical security policy preventing unauthorized physical access to the UCS. The policy must document physical security controls including access control, physical separation of hardware, and monitoring policies to ensure no unauthorized physical access to the UCS system is allowed.
- The facility housing the UCS system must have a power management strategy using UPS or backup generators to ensure that power continues to flow under any adverse conditions.
- The network connectivity feeding the UCS system in the datacenter must provide redundant links to protect against network administrator operator error or network equipment failure.
- An authentication for remote authentication of TOE administrators may be available, if so communications from the TOE to the remote authentication server shall be protected.

4.1 Clarification of Scope

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

- The Cryptography used by the product has not been independently certified. The Cryptography of the product is vendor certified to operate correctly.
- Administrators must be careful when dealing with audit records. The storage capacity for each log type is 10,000 records, and is not configurable. When each log reaches capacity, the oldest records are overwritten by new records. To ensure there is no loss of audit data, the administrator must export audit data in a timely manner. There are no alerts provided when audit data is overwritten.

5 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

5.1 TOE Introduction

The TOE consists of a minimum of one of each of the following components:

- Cisco UCS Manager components
  - One or more Cisco UCS 6120XP, or 6140XP, or 6248UP Fabric Interconnects with
    - Cisco UCS Manager Software release 1.4(1m)
- Server and Fabric Extenders (chose blade and/or rack mount)
  - Blade server configurations:
    - One or more Cisco UCS 5108 Chassis with:
      - One or more Cisco UCS 2104XP Fabric Extenders
      - One or more Cisco UCS B200 M1, B200 M2, B230 M1, B250 M1, B250 M2, or B440 M1 Blade Servers; and/or
  - Rack-Mount Server configurations:
    - One or more Cisco Nexus 2248TP Fabric Extenders
    - One or more Cisco UCS C200 M1, C200 M2, C210 M1, C210 M2, C230 M1, C230 M2, C250 M1, C250 M2, C260 M2, C460 M1, or C460 M2 Rack-Mount Servers

Deployment note: One instance of the Cisco UCS Manager can manage two Cisco UCS 6100 Series Fabric Interconnects, multiple Cisco UCS 5100 Series Chassis, 80 Cisco UCS 2100 Series Fabric Extenders, and hundreds of Cisco UCS B-Series Blade Servers and/or Rack-Mount Servers. [Capacity details are provided for conceptual purposes only, and are not tested within the scope of the Common Criteria evaluation.]

5.2 Cisco UCS 5108 Chassis

The Cisco UCS 5108 Chassis physically houses blade servers and up to two fabric extenders. The enclosure is 6RU high supporting up to 56 servers per rack density. The UCS 5108 supports up to eight half slot or four full slot blade servers with four power supplies and eight cooling fans. Both power supplies and fans are redundant and hot swappable. Featuring 90%+ efficient power supplies, front to rear cooling, and airflow optimized mid-plane, the Cisco UCS is optimized for energy efficiency and reliability.

Even though the Blade Server Enclosure and Cisco UCS System can house multiple blades, each blade acts as an individual physical server. Cisco UCS System provides a centralized and simplified management paradigm for all the blades.

5.3 Cisco UCS 6120XP and 6140XP Fabric Switch Hardware

The Cisco UCS 6120XP and 6140XP Fabric Switch Hardware are line-rate, low-latency, lossless 10 Gigabit Ethernet, Cisco Data Center Ethernet, and Fiber Channel over Ethernet (FCoE) switches that consolidate I/O at the system level. The Fabric Switches supply a unified network fabric that connects every server resource in the system via wire once 10G Ethernet/FCoE downlinks and 10G Ethernet and 1/2/4Gb FC uplink modules are configured. Out of band management, switch redundancy, and console-based diagnostics are enabled through dedicated management, clustering, and RS-232 ports. A single UCS Series Fabric Switch unites up to 320 servers within a single system domain for maximum scalability.

The Cisco UCS Series Fabric Switch has two flavors – a 1RU switch and a 2RU switch. The 2RU Fabric switch supports 40 fixed 10G FCoE ports and 2 expansion modules. It supports redundant power supplies and fans and a front-to-back airflow. The 1RU Fabric switch supports 20 fixed 10G FCoE ports and 1 expansion module. It supports redundant power supplies and fans and a front-to-back airflow.

The external authentication server can act as a repository for authentication credentials. The Cisco UCS Fabric switch implements SSHv2, SNMPv3 and SSL3.1/TLS1.0 for secure network management. The expansion modules supported on the Cisco UCS Fabric Switch include a 6-port Enhanced 10-Gbit Ethernet interface expansion module, a 4-port Enhanced 10-Gbit Ethernet interface and 4-port 1/2/4Gbps Fibre-Channel expansion module and a 8-port 1/2/4Gbps Fibre-Channel expansion module.

5.4 Cisco UCS 2104XP Fabric Extender

The Cisco UCS 2104XP Series Fabric Extender extends the I/O fabric into the blade server enclosure providing a direct 10Gbs connection between blade servers and fabric switch simplifying diagnostics, cabling, and management. The fabric extender multiplexes and forwards all traffic using a cut-through architecture over one to four 10Gbps unified fabric.

5.5 Cisco UCS Blade Servers

Cisco UCS B200 M1, B200 M2, B230 M1, B250 M1, B250M2, and B440 M1 Blade Servers are designed for compatibility, performance, energy efficiency, large memory footprints, manageability, and unified I/O connectivity. Based on Intel® Xeon® 5500 series processors, B-Series Blade Servers adapt to application demands, scale energy use, and offer a platform for virtualization. Each Cisco UCS B-Series Blade Server utilizes converged network adapters for consolidated access to the unified fabric with various levels of transparency to the operating system. This design reduces the number of adapters, cables, and access-layer switches for LAN and SAN connectivity at the rack level.

The Blade Servers include a Cisco Integrated Management Controller (CIMC). The CIMC provides access to the Server for UCS at the BIOS level via the Intelligent Platform Management Interface (IPMI) that can be used to monitor system health at the hardware level and manage the server's firmware[1]. Configuration changes to the BIOS for the server can be requested through the CIMC; however the CIMC is not available for direct management use.

The Blade Servers have nine options for network adapters:

- Cisco UCS M81KR Virtual Interface Card
- Cisco UCS 82598KR-10 Gigabit Ethernet Network Adapter
- Cisco UCS M71KR-Q QLogic Converged Network Adapter
- Cisco UCS M72KR-Q Qlogic Converged Network Adapter
- Cisco UCS M71KR-E Emulex Converged Network Adapter
- Cisco UCS M72KR-E Emulex Converged Network Adapter
- Cisco UCS M81KR Virtual Interface Card
- Cisco UCS M61KR-I Intel Converged Network Adapter
- Cisco UCS NIC M51KR-B Broadcom BCM57711 Network Adapter

A table that compares the adapters can be found at:
http://www.cisco.com/en/US/prod/ps10265/ps10280/cna_models_comparison.html.

5.6 Cisco UCS Rack Mount Servers

Cisco UCS C200 M1, C200 M2, C210 M1, C210 M2, C230 M1, C230 M2, C250 M1, C250 M2, 260 M2, C460 M1, and C460 M2 Rack-Mount Servers extend UCS functionality to an industry-standard form factor and are designed for compatibility, and performance, and enable organizations to deploy systems incrementally, using as many or as few servers as needed.
The Rack-mount Servers include a Cisco Integrated Management Controller (CIMC). The CIMC provides access to the Server for UCS at the BIOS level via the Intelligent Platform Management Interface (IPMI) that can be used to monitor system health at the hardware level and manage the server's firmware[2]. Configuration changes to the BIOS for the server can be requested through the CIMC. The C-Series servers are managed through the UCSM, which interfaces with the CIMC.

The Rack Mount Servers have nine options for network adapters:

- Cisco UCS P81E Virtual Interface Card
- Cisco UCS M81KR Virtual Interface Card
- Emulex OneConnect Universal Converged Network Adapter

[1] Blade server firmware is outside the scope of the TOE. Blade server firmware does not provide any security functionality described in this Security Target, and is not part of in the UCSM software bundle.
[2] Blade server firmware is outside the scope of the TOE. Blade server firmware does not provide any security functionality described in this Security Target, and is not part of in the UCSM software bundle.

- QLogic QLE8152 Dual Port 10 Gb Ethernet to PCIe Converged Network Adapter
- Cisco UCS CNA M61KR-I Intel Converged Network Adapter
- Broadcom NetXtreme II 5709 Quad Port Ethernet PCIe Adapter Card with TOE and iSCSI HBA
- Broadcom NetXtreme II 57711 Dual Port 10 Gb Ethernet PCIe Adapter Card with TOE and iSCSI HBA
- Emulex LightPulse LPe11002 4 Gbps Fibre Channel PCI Express Dual Channel HBA
- QLogic SANblade QLE2462, Dual Port 4 Gbps Fibre Channel to PCI Express HBA

None of the functionality described is security enforcing.

5.7 Cisco UCS Manager Software

The Cisco UCS Manager Software integrates the components of a Cisco Unified Computing System into a single, seamless entity. It can manage up to three hundred and twenty blade servers as a single logical domain using a GUI, with both CLI and XML API options, enabling near real time configuration and reconfiguration of resources.

The software's role-based design supports existing best practices, allowing server, network, and storage administrators to contribute their specific subject matter expertise to a system design. Any user's role may be limited to a subset of the system's resources using organizations and locales, so that a Cisco Unified Computing System can be partitioned and shared between organizations using a multi-tenant model. It allows secure management of the TOE using SSL3.1/TLS1.0, SNMPv3 and SSHv2.

The UCS Manager software is divided into two components: server and client side. The server side component is installed on the 6120XP or 6140XP Fabric Switch hardware. The server side component contains the XML based server daemon that receives requests from the three different client access methods: GUI, CLI, and XML. The client side component is a java application that provides the GUI for the administrator.

- The UCS Manager software may be deployed in a standalone configuration, in which each instance of the TOE is managed independently, or in a clustered configuration in which management configuration data and event log storage are centralized in a primary TOE instance and accessed by the other members of the cluster. Clusters operate within the protected network boundary.

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco Unified Computing System. Only those documents identified in the Guidance Documentation section are provided to customers.

6.1 Design Documentation

1. Cisco Unified Computing System Security Architecture Specification, Version 0.5, July 19, 2011
2. Cisco Unified Computing System Functional Specification, Version 0.4, July 8, 2011
3. Cisco Unified Computing System TOE Design Specification, Version 0. 3, March 1, 2011
4. Cisco Unified Computing System Functional Specification Annex B RFC Security Parameter Relevancy, July 7, 2011

6.2 Guidance Documentation

1. Cisco Unified Computing System (UCS), version 1.4(1m) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5, October 2011
2. Cisco UCS Site Preparation Guide; July 2009
3. Release Notes for Cisco UCS Software, Release 1.4; First Published: December 19, 2010; Last Updated: September 2, 2011; Part Number: OL-2408-01
4. Cisco UCS Manager CLI Configuration Guide, Release 1.4; First Published: December 07, 2010; Last Modified: April 27, 2011
5. Cisco UCS Manager CLI Command Reference, Release 1.4; First Published: December 19, 2010; Last Modified: April 15, 2011
6. Cisco UCS Manager GUI Configuration Guide, Release 1.4; First Published: December 07, 2010; Last Modified: April 27, 2011
7. Use UCS Manager GUI to Manage Cisco UCS; Document ID: 110474
8. Set up Role−Based Access Control in Cisco UCS; Document ID: 110241
9. Set up RADIUS Authentication for Cisco UCS; Document ID: 110521
10. Setup TACACS Authentication for Cisco UCS; Document ID: 110520
11. Set up Syslog for Cisco UCS; Document ID: 110265
12. Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide; January 25, 2010; Part Number: OL-20036-02
13. Set up Connectivity between Fabric Extender and Fabric Interconnect in UCS; Document ID: 110296
14. Cisco UCS B-Series Servers Documentation Roadmap

15. Cisco UCS 5108 Server Chassis Hardware Installation Guide, April 4, 2010
16. Cisco UCS B200 Blade Server Installation and Service Note; Part number: OL-22473-02
17. Cisco UCS B250 Extended Memory Blade Server Installation and Service Note; Part Number: OL-22474-02
18. Unified Computing System KVM Console Access to Blade Server Configuration Example; Document ID: 110435; Updated: Apr 28, 2010
19. LAN and SAN Connectivity for a Cisco UCS Blade; Document ID: 110202; Updated: Sep 02, 2009
20. Cisco UCS B-Series Blade Servers Linux Installation Guide; December 07, 2010
21. Cisco UCS B-Series Blade Servers VMware Installation Guide; October 06, 2010
22. Cisco UCS B-Series Blade Servers Windows Installation Guide; October 06, 2010
23. Cisco UCS C-Series Servers Documentation Roadmap; Part Number: OL-21120-02
24. Cisco UCS C200 Server Installation and Service Guide, Covers UCS C200 Server Generations M1 and M2; August 31, 2011
25. Cisco UCS C210 Server Installation and Service Guide, Covers UCS C210 Server Generations M1 and M2; November 11, 2010
26. Cisco UCS C250 Server Installation and Service Guide, Covers UCS C250 Server Generations M1 and M2; November 11, 2010
27. Cisco UCS Server Configuration Utility, Release 1.0 For Cisco UCS C-Series Servers
28. Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.4(1); First Published: September 02, 2011, Text Part Number: OL-23490-04
29. Cisco UCS C-Series Servers Integrated Management Controller CLI Command Reference, Release 1.4(1); First Published: September 06, 2011, Text Part Number: OL-23494-04
30. Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.4(1); First Published: September 06, 2011, Text Part Number: OL-23489-04
31. Cisco UCS C-Series Servers Linux Installation Guide; December 07, 2010
32. Cisco UCS C-Series Servers VMware Installation Guide; August 11, 2010
33. Cisco UCS C-Series Servers Windows Installation Guide; August 11, 2010
34. Cisco UCS Manager B-Series Troubleshooting Guide; July 11, 2011
35. Cisco UCS Faults Reference; July 13, 2010; Revised: April 21, 2011
36. Cisco UCS RAID Controller SMI-S Reference Guide; Release 1.0; June 16, 2010
37. Cisco UCS SMASH Reference Guide; Release 1.0; June 15, 2010
38. Cisco UCS Manager XML API Programmer's Guide; March 31, 2010

39. Cisco UCS MIB Quick Reference; Release Date: July 9, 2010; Text Part Number: OL-20152-02

40. Intelligent Platform Management Interface Specification Second Generation v2.0

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco Unified Computing System (UCS), Reference: UCS-CMP-v2-0, October 2011, Version: 2.0

1. Development Security for Cisco Unified Computing System (UCS), Reference: UCS-DVS-v1-0, September 2010, Version: 1.0

6.4 Testing

1. UCSM Common Criteria Test, Revision 5, August 9, 2011
2. UCS CC ATE_FUN ATE_COV ATE_DPT-20110809-kd.xls, August 9, 2011
3. Actual Test Results
    a. AUDIT_LOG-11.1.doc
    b. Cryptography-11.8.doc
    c. HA-11.6.doc
    d. IMPI-11.5.doc
    e. Miscellenious-11.7.doc
    f. RBAC_11.2.x_Results.doc
    g. VLAN-11.3.doc

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco Unified Computing System (UCS), Version 2.0, November 11, 2011.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

1. Audit
2. Identification & Authentication
3. Management
4. Network Separation
5. Role Based Access Control

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Common Criteria Guide, ran a sample of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing boundary conditions not tested by Cisco. The evaluation team tested combinations of the information flow policies that Cisco did not test. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Cisco Unified Computing System (UCS) including:

- Hardware models - Cisco UCS 5108 Blade Server Chassis, Cisco UCS B200 M1 and M2, B230 M1, B250 M1 and M2, and B440 M1 Blade Servers, Cisco UCS C200 M1 and M2, C210 M1 and M2, C250 M1 and M2, C260 M2 and C460 M1 and M2 Rack-Mount Servers, Cisco UCS 6120XP, and 6140XP Fabric Interconnects, Cisco UCS 2104XP, and 2248TP Fabric Extenders
- Software versions - Cisco Unified Computing System (UCS) Manager Software 1.4(1m)

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Unified Computing System (UCS) Common Criteria Operational User Guidance and Preparative Procedures, October 2011** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 3 and CEM version 3.1 rev 3. The evaluation determined the Cisco Unified Computing System (UCS) TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Unified Computing System (UCS) solution that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a detailed design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally,

the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team re-ran the entire vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Cisco Unified Computing System meets the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The Cryptography used by the product has not been independently certified. The Cryptography of the product is solely vendor certified to operate correctly. No FIPS or CAVP evaluations of the cryptography have been performed.
- Administrators must be careful when dealing with audit records. The storage capacity for each log type is 10,000 records, and is not configurable. When each log reaches capacity, the oldest records are overwritten by new records. To ensure there is no loss of audit data, the administrator must export audit data in a timely manner. There are no alerts provided when audit data is overwritten.
- The evaluation team observed that the vendor's security tests are predominantly manual and apparently not closely integrated with the extensive automated testing performed as a routine part of product development. While these evaluated tests are sufficient to satisfy Common Criteria requirements, the validation team recommends a closer integration in future efforts, in order to improve test integration and provide greater test coverage.
- Although the vendor apparently maintains a significant internal organization responsible for vulnerability analysis and flaw remediation, the evaluation team was not provided access to any of that organization's personnel or to the vulnerability reports and analysis performed therein. Again, while the materials provided are sufficient to satisfy the conformance requirements for vulnerability analysis and flaw remediation, the validation team considers the lack of access a lost opportunity to assess and describe the details of analysis and remediation work performed by the vendor.
- Syslog is required to ensure complete auditing of some key functions; however, syslog is disabled by default during installation. It is important for users to manually enable syslog in accordance with the CC user's OPE guide to ensure proper auditing.

11 Security Target

The Security Target is identified as *Cisco Unified Computing System (UCS) Security Target, Version 1.0,* December 2011. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.2.

12 Glossary

The following abbreviations and definitions are used throughout this document:

CC ……..……Common Criteria
EAL4 ……..……Evaluation Assurance Level 4
IT ……..……..Information Technology
NIAP ……..……..National Information Assurance Partnership
PP ……..……Protection Profile
SF ……..……Security Function
SFP ……..……..Security Function Policy
ST ……Security Target
TOE ……..……Target of Evaluation
TSC ……..……TSF Scope of Control
TSF ……..……..TOE Security Functions
TSFI ……TSF Interface
TSP ……..……TOE Security Policy

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 3, dated: July 2009.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 3, dated: July 2009.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 3, dated: July 2009

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 3, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Unified Computing System (UCS) Part 1 (Non-(Proprietary)*, Version 1.0, November 11, 2011

[7] Science Applications International Corporation. *Evaluation Technical Report for the Unified Computing System (UCS) Part 2 (Proprietary)*, Version 2.0, November 11, 2011.

[8] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco Unified Computing System (UCS)*, Version 2.0, September 23, 2011. NOTE: This document was used only to develop summary information regarding the testing performed by the CCTL.

[9] Cisco Unified Computing System Security Target, Version 1.0, December, 2011.