ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 Security Target

Date: *April 13, 2026*
Version: *0.18*
Prepared By: *Dawn Adams*
Prepared For: *OpenText*
275 Frank Tompa Drive
Waterloo ON N2L 0A1
Canada

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

1. Introduction: 5
   1.1. Security Target Reference: 5
   1.2. TOE Reference:v0.2 of the 5
   1.3. Document Organization: 5
   1.4. Document Terminology: 6
   1.5. Document Conventions 6
   1.6. TOE Overview: 7
      1.6.1. ArcSight Management Center (ArcMC) 7
      1.6.2. ArcSight SmartConnectors 8
   1.7. TOE Description: 8
      1.7.1. Overview: 8
      1.7.2. TOE Components and Environment Requirements: 9
      1.7.3. TOE Usage: 10
      1.7.4. TOE Component Descriptions 10
      1.7.5. Physical Boundary 11
      1.7.6. Logical Boundary: 11
      1.7.7. TOE Delivery: 12
      1.7.8. TOE Guidance: 14
      1.7.9. Supported Functionality Excluded from the Evaluated Configuration: 14
2. CC Conformance Claim: 15
   2.1. PP Claim 15
   2.2. Package Claim 15
   2.3. Conformance Rationale 15
3. Security Problem Definition 16
   3.1. Threats 16
   3.2. Organizational Security Policies 16
   3.3. Assumptions 16
4. Security Objectives 18
   4.1. Security Objectives for the TOE 18
   4.2. Security Objectives for the Operational Environment 18
   4.3. Security Objectives Rationale 19
      4.3.1. Mapping of Objectives: 19

5. Extended Components Definition 21
6. Security Requirements 22
6.1. Document Conventions 22
6.2. Security Functional Requirements 22
6.3. Security Audit (FAU) 23
6.3.1. FAU_GEN.1 Audit Data Generation 23
6.3.2. FAU_SAR.1 Audit Review 24
6.3.3. FAU_SAR.2 Restricted Audit Review 24
6.3.4. FAU_SAR.3 Selectable Audit Review 24
6.3.5. FAU_STG.2 Protected Audit Data Storage 24
6.4. Cryptographic Support (FCS) All provided by the environment 24
6.4.1. FCS_CKM.1 Cryptographic Key Generation 24
6.4.2. FCS_CKM.3 Cryptographic Key Access (N/A) 25
6.5. FCS_CKM.6 Timing and Event of Cryptographic Key Destruction 25
6.5.1. FCS_RBG.1 Random bit generation (RBG) 25
6.5.2. FCS_RBG.2 Random bit generation (external seeding) 25
6.5.3. FPT_FLS.1 Failure with preservation of secure state 25
6.5.4. FPT_TST.1 TSF Self-Test 25
6.6. FCS_COP.1 Cryptographic Operation 26
6.7. Identification and authentication (FIA) 26
6.7.1. FIA_AFL.1 Authentication Failure Handling 26
6.7.2. FIA_ATD.1 User Attribute Definition 26
6.7.3. FIA_UAU.2 User Authentication before Any Action 26
6.7.4. FIA_UID.2 User Identification before Any Action 26
6.8. Protection of the TSF (FPT) 27
6.8.1. FPT_ITT.1 Basic internal TSF data transfer protection 27
6.9. Security Management (FMT) 27
6.9.1. FMT_MOF.1 Management of security functions behaviour 27
6.9.2. FMT_MTD.1 Management of TSF Data 27
6.9.3. FMT_SMF.1 Specification of Management Functions 27
6.9.4. FMT_SMR.1 Security Roles 27
6.10. TOE Access (FTA) 27
6.10.1. FTA_SSL.3 TSF-initiated termination 27

6.10.2. FTA_SSL.4 User-initiated termination 27
6.11. Trusted Path / Channel 28
6.11.1. FTP_TRP.1 Trusted Path 28
6.11.2. FTP_ITC.1 Inter-TSF trusted channel 28
6.12. Security Assurance Requirements 28
6.13. Security Assurance Requirements Rationale 29
6.14. Security Requirements Rationale 29
6.14.1. Dependency Rationale 29
6.14.2. Security Functional Mappings 31
6.14.3. Sufficiency of Security Requirements 32
7. TOE Summary Specification 34
7.1. TOE Security Functions 34
7.2. Security Audit 34
7.3. Cryptographic Support 34
7.4. Identification and Authentication 35
7.5. Security Management 35
7.6. Protection of the TSF 36
7.7. TOE Access 36
7.8. Trusted Path 36

1. Introduction:

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, the TOE overview and TOE Description.

The ST contains the following additional sections:

- Conformance Claims (Section 2)— claims of conformance to CC2022.
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational
- environment necessary to counter the threats and satisfy the assumptions that define the security problem
- Extended Requirements – (Section 5) – specifies whether any SFRs or SARs are extended
- IT Security Requirements (Section 6)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 7)—describes the security functions of the TOE and how they satisfy the SFRs

1.1. Security Target Reference:

ST Title	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 Security Target
ST Revision	0.18
ST Publication Date	April 13, 2026
Author	Dawn Adams

1.2. TOE Reference:

TOE Reference	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1

Note: This document also makes reference to the TOE or just ArcMC and Connectors. Both also refer to ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1.

1.3. Document Organization:

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable

SECTION	TITLE	DESCRIPTION
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4. Document Terminology:

The following table describes the acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version 2022
DB	Database
EAL	Evaluation Assurance Level
EOE	Events Originating External to the TOE
FIPS	Federal Information Processing System
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
ISO	International Standards Organization.
LDAP	Lightweight Directory Access Protocol
OSP	Organizational Security Policy
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network

Table 2 – Acronyms Used in Security Target

1.5. Document Conventions

Security Functional Requirements in CC2022 defines the approved set of operations that may be applied to functional requirements: iteration; assignment; selection; and refinement.

Iteration—allows a component to be used more than once with varying operations. In this ST,

iteration is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).

Assignment—allows the specification of an identified parameter. Assignments are indicated using text enclosed by brackets (e.g., [assignment]).

Selection—allows the specification of one or more elements from a list. Selections are indicated using italics and are enclosed by brackets (e.g., [selection]).

Refinement—allows the addition or removal of details. Refinements are indicated using bold, for additions, and strike-through, for deletions.

1.6. TOE Overview:

The TOE is the ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 from OpenText. Communications between the ArcMC and browser are protected by TLS v1.2 supplied by the Voltage Cryptographic Module (CMVP certificate #2686). The communications between the ArcMC and SmartConnectors and between the ArcMC and trusted IT products are protected by TLS v1.2 provided buy Bouncy Castle 2.1.0 (CMVP certificate # 4943).

1.6.1. ArcSight Management Center (ArcMC)

The ArcSight Management Center (ARcMC) is a a centralized management tool that supports security policy configuration, deployment maintenance, and monitoring. It provides a single management interface to administer ArcMC managed nodes, including Loggers, SmartConnectors, Event Brokers, and other ArcMCs.

ArcMC provides a browser-based graphical user interface (GUI). The browsers that are supported are:
MicrosoftEdge(latest version)
Firefox ESR(latest version)
Google Chrome(latest version)

The GUI enables ArcMC users to access the following functional capabilities:

- Manage the following node types:
  - o SmartConnectors
  - o Hardware or Software Loggers
  - o Event Brokers
  - o ArcSight Management Centers
- Create and manage node configurations
- View status of all nodes being managed
- Manage users across all managed nodes
- Administer ArcMC itself
- View statistics of total Events Per Second (EPS) in and out from all managed connectors.

ArcSight ArcMC and SmartConnectors is a log management solution designed to handle high event throughput, support data analysis, and provide efficient long-term storage.

1.6.2. ArcSight SmartConnectors

SmartConnectors both receive and retrieve information from network devices. If the device sends information, the SmartConnector becomes a receiver. But, if the device does not send information, the SmartConnector can retrieve it. SmartConnectors are also available to forward events between ArcSight systems such as Transformation Hub and ESM (other OpenText products that are not included in this evaluation), enabling the creation of multi-tier monitoring and logging architectures for large organizations and Managed Service Providers.

ArcSight SmartConnectors collect and process events generated by devices throughout an enterprise. Devices can be routers, e-mail logs, anti-virus products, firewalls, Intrusion Detection Systems, access control servers, VPN systems, anti-DoS appliances, operating system logs, and other sources where information of security threats are detected and reported.

SmartConnectors are specifically developed to work with network and security products using multiple techniques, including simple log forwarding and parsing, direct installation on native devices, SNMP, and syslog.

The following specific SmartConnectors were tested as part of the evaluated configuration:
• Syslog NG Daemon—can collect syslog records from Syslog NG Daemon, an open source implementation of the syslog protocol for UNIX and UNIX-like systems that extends the original syslogd model.
• Microsoft Windows Event Log – Native (WINC)—collects Windows Event Log events.
• Linux SmartConnector

Other SmartConnectors may be deployed in an evaluated configuration, but no conclusions should be drawn regarding the efficacy of their event collection functionality.

1.7. TOE Description:

1.7.1. Overview:

The TOE consists of the following components:
ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1

The TOE uses HTTPS/TLS provided by the environment to communicate with TOE Elements. The TOE supports TLS v1.2.

Between the Browser and ArcMC the encrypted link is provided by Voltage Cryptographic Module v5.0 This is FIPS 140-2 validated (Certificate #2686). Between ArcMC and the SmartConnectors, the TLS 1.2 link is provided by Bouncy Castle v2.1.0. Between ArcMC and the

trusted IT products the TLS 1.2 ciphers are also provided by Bouncy Castle v2.1.0. This Bouncy Castle is FIPS 140-3 validated (Certificate # 4943).

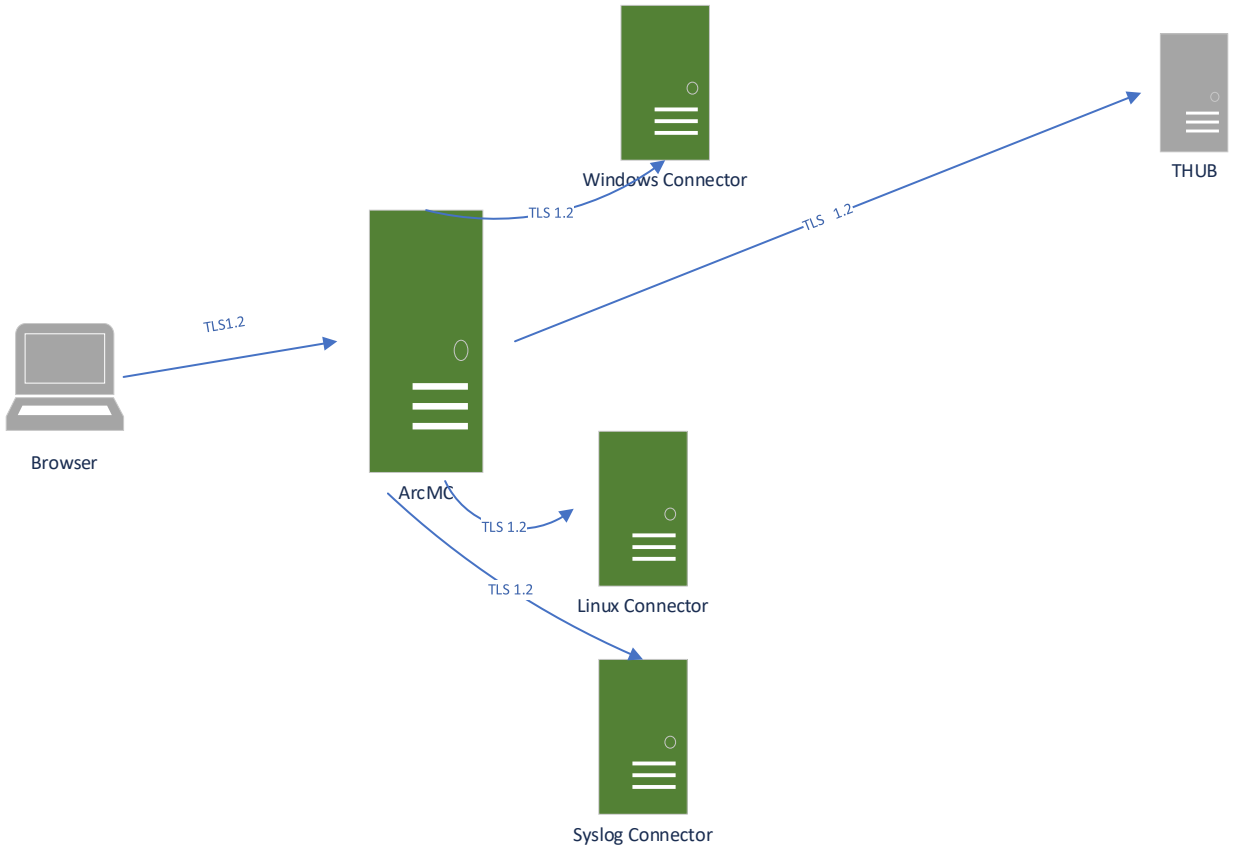


Figure 1 - TOE evaluated configuration

1.7.2. TOE Components and Environment Requirements:

The configuration requirements for the operational environment to support the TOE are listed in the table.

ArcMC Version	Support	Operating System
3.2.5	MF Tested Supported	Red Hat Enterprise Linux (RHEL) 9.2,8.8,7.9. Rocky Linux 9.2, 8.8
SmartConnector Version	Support	Operating System
8.5.1	MF tested	RHEL 8.6 and 9.2 Rocky Linux 8.9 CentOS Linux 7.9

		Oracle Solaris 11, 64-bit MS Windows Server 2022 Standard 64-bit SUSE Linux Enterprise Server (SLES) 15 SP 5
	Supported	CentOS Linux 8.x and 7.x 64-bit RHEL 9.x, 8.x and 7.x 64 bit MS Windows Server 2022 Standard 64 bit MS Windows Server 2019 Standard 64 bit MS Windows Server 2016 Standard 64 bit MS Windows Server 2012 R2 Standard 64 bit Oracle Solaris 11, 64 bit (SPARC) Oracle Solaris 10, 64 bit (SPARC) Oracle Solaris 11, 64 bit (x86_64) SUSE Linux Enterprise Server 15 SP 3, 15 SP2, 15 SP1, 15, 12 SP2 and 11 64-bit

Table 3: Tested/Supported ArcMC and SmartConnector Environments

Micro Focus tested means the TOE has been tested by Micro Focus and is Micro Focus "certified". The other listed OSs are supported but are not fully tested.

For the evaluation the IT environment also requires the following software component:
THUB

1.7.3. TOE Usage:

ArcMC is a management tool that manages and ArcSight software such as SmartConnectors, Logger, Transformation Hub and other ArcMCs. Transformation Hub and Logger are not part of this evaluation. SmartConnectors format the data they retrieve into a useable format that can be sent to ArcMC.

1.7.4. TOE Component Descriptions

1.7.4.1. ArcMC

Arcsight Management Center (ArcMC) is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost effective manner. ArcMC offers these key capabilities:

- Management and Monitoring: deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Connector Appliances, Loggers, Connectors, Collectors, other ArcMCs, and Transformation Hub.
- SmartConnector Hosting: for the hardware appliance, as a platform to host and execute SmartConnectors ArcMC includes these benefits:
  - i) Rapid implementation of new and updated security policies. l Increased level of accuracy and reduction of errors in configuration of managed nodes
  - ii) Reduction in operational expenses.

1.7.4.2. SmartConnectors

Note that individual SmartConnectors run only on the platforms that are useful for the connector type and specific device type. For example, the SmartConnector for Microsoft Windows Event Log runs on Windows platforms only. Each SmartConnector has its own specific configuration guide that provides connector-specific platform requirements and installation information.

SmartConnectors can:

- Collect all the data from a source device, which eliminates the need to return to the device during an investigation or audit.
- Parse individual events and normalize event values such as severity, priority, and time zone into a common schema (format) for use by other products.
- Filter out data that is not needed for analysis, thus saving network bandwidth and storage space (optional).
- Filter and aggregate events to reduce the volume sent to the Manager, ArcSight Logger, or other destinations, which reduces event processing time and increases efficiency of ArcSight.
- Categorize events by using a common, human-readable format, saving time, and making it easier to use the event categories to build filters, rules, reports, and data monitors.
- Add device and event information to it to complete the message and send it to the configured destination.

Data Encryption

Connectors provide the OpenText Voltage Cryptographic Module v5.0 format-preserving encryption to adhere to the regulatory requirement, which mandates that data leaving the SmartConnector machine to another destination must be encrypted. This feature is supported only on Linux and Windows 64-bit platforms.

The Configuration Guide for the specific SmartConnector has information about the format preserving parameters for SmartConnectors.

1.7.5. Physical Boundary

The ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 comprise the TOE. The evaluated configuration requires a THUB server.

1.7.6. Logical Boundary:

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

TSF	DESCRIPTION
Security Audit	ArcMC is able to generate and store audit records of security-relevant events. The stored audit records are protected from unauthorized modification and deletion. Audit records generated by ArcMC can be viewed only by users in the System Admin role. ArcMC provides the authorized roles with capabilities to review the generated audit records, including capabilities for selecting audit records based on date and time range and, optionally, subject identity and outcome, and ordering the selected records based on date and time, the subject associated with the audit event, and the type of audit event.
Cryptographic Support	Cryptography for TLS connections is supplied by the operational environment. Communications between the TOE and trusted IT entities are protected by TLS v1.2. Format preserving encryption is provided for data encryption by Voltage Cryptographic Module.
Identification and Authentication	The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user identity; authentication data; authorizations (groups or roles); and e-mail address information. The TOE supports both passwords and certificates for authentication and users can be configured for password-only, certificate-only, or password and certificate-based authentication. The TOE additionally supports external LDAP and RADIUS authentication servers. The TOE enforces restrictions on password structure, including minimum length and minimum number of different character types (i.e., alphabetic, numeric, special). The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE is granted.
Security Management	ArcMC provides authorized users with a GUI that can be used to configure and manage ArcMC security functions and TSF data, depending on the security management roles assigned to the user.
Protection of the TSF	Communications between distributed components of the TOE occur over TLS provided by the environment, which provides confidentiality and integrity of transmitted data.
TOE Access	The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off. The content of the message can be configured by an administrator.
Trusted Path / Channels	The TOE provides a trusted path/channel to communicate securely with the TOE and between separate pieces of the TOE. This is implemented using HTTPS (i.e., HTTP over TLS). The cryptography is provided by the environment. Communications with Transformation Hub are also The use of HTTPS ensures all communication over the trusted path/channel is protected from disclosure and modification.

Table 5 – Logical Boundary Descriptions

1.7.7. TOE Delivery:

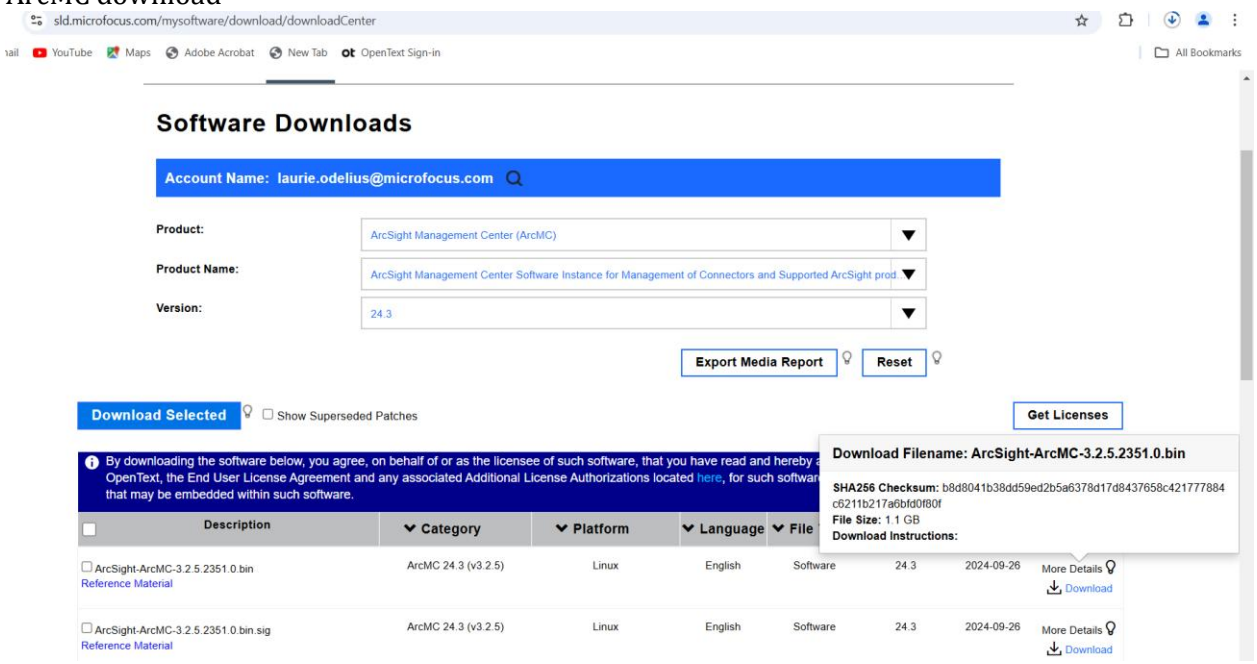
The TOE software is provided to customers via secure download from the download portal (https://sld.microfocus.com/mysoftware/index)The software is available as an iso formatted optical disk (.iso). Once downloaded, the ISO files can be expanded to perform the installation.

Protected by HTTPS.

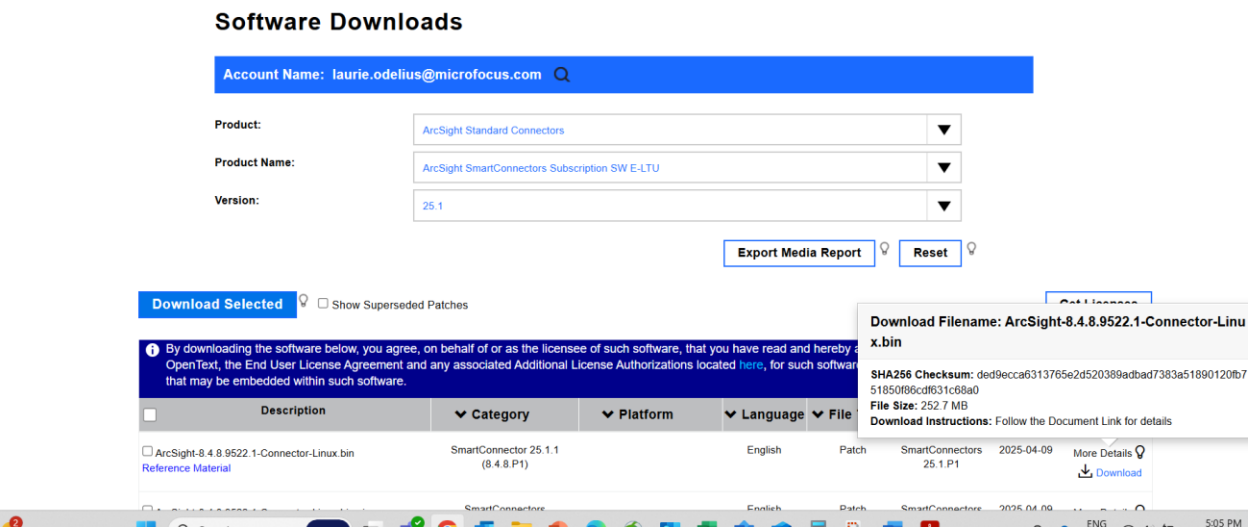
The installer file for ArcSight ArcMC is: ArcSight-ArcMC-3.2.5.2351.bin

SmartConnectors are provisioned in a single installer file from which the desired SmartConnectors are selected and installed.

ArcMC download



SmartConnector download



1.7.8. TOE Guidance:

The TOE includes the following guidance documentation:
Micro Focus Arcsight Management Center Software Version: 3.0.0 Administrator's Guide
Micro Focus Security ArcSight SmartConnector Software Version: 25.1 SmartConnector Installation and User Guide.
The documentation is available on the web in either html or pdf formats. For addition information please see the product guidance documents.

Additional TOE operational guidance and installation procedures will be provided in the TOE Operational Guidance and Installation Procedures (AGD-IGS.1).

As OpenText moves to new nomenclature for its products, documentation and downloads, the versioning should be CE YY.x. CE is Cloud Edition. As of today, the versioning is:
Product version: ArcMC CE 24.3 and SmartConnectors CE 25.4
Product documentation: ArcMC CE 24.3 and SmartConnectors CE 25.4
CC documentation: ArcMC CE 24.3 and SmartConnectors CE 25.4
Download files: ArcMC 3.2.5 and SmartConnectors 8.5.1

1.7.9. Supported Functionality Excluded from the Evaluated Configuration:

- Hadoop functionality

2. CC Conformance Claim:

The TOE is conformant to Common Criteria Version CC:2022 Revision 1 November 2022.

The CC standard documents are:
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 4: Framework for the specification of evaluation methods and activities Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 5: Pre-defined packages of security requirements

The TOE is conformant to: CC Part2 conformant and CC Part3 conformant.

2.1. PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.2. Package Claim

The TOE claims conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version CC:2022. The TOE does not claim conformance to any functional package. The TOE EAL3 assurance package is augmented with ALC_FLR.3.

2.3. Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

EAL3+ was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3+ provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

The product was augmented to comply with ALC_FLR.3 in order to document and address requirements for remediation and reporting of faults that may be discovered in the product after release. The TOE invokes the Environment cryptography to establish TLS1.2 channels for secure communications.

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1. Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration. The asset is the configuration of the TOE.
T.NO_PRIV	An authorized user of the TOE exceeds their assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data. The assets are the: - audit data that is collected - configuration of the TOE - privileges / rights / roles assigned to users - stored credentials
T.SENSDATA	An unauthorized user may be able to view sensitive data passed between the TOE and its remote users, and between the TOE components, and exploit this data to gain unauthorized privileges on the TOE.

Table 6 – Threats Addressed by the TOE

3.2. Organizational Security Policies

There are no Organisational Security Policies for this TOE.

3.3. Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.AUDIT_PROTECT	The Audit data is protected from modification and disclosure.
A.HTTPS	HTTPS using TLS is used to access the TOE. The TOE uses environment Crypto to communicate with parts of the TOE and trusted IT products.
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.

ASSUMPTION	DESCRIPTION
A.MANAGE	Privileged users (Administrators and Users) of the TOE are assumed to be appropriately trained (and competent) to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Privileged users (Administrators, Users) of the TOE, are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Privileged Users (Administrators and Users) will not leave their systems unattended and unlocked.
A.TIMESOURCE	The TOE has a trusted source for system time via the OS.
A.UPDATE	The TOE environment is patched by the administrator as patches are available to minimize the effects of vulnerabilities that may arise.

Table 7 – Assumptions The TOE, and the TOE environment are regularly updated by an administrator to address potential and actual vulnerabilities.

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUDIT	The TOE shall collect audit data from TOE activities including changes to permissions, privileges, roles, rules, and provisioning of access.
O.PRIVILEGE	The TOE must protect stored credentials from disclosure.
O.SEC_ACCESS	The TOE shall ensure that only Administrators and authorized applications are granted access to security functions, configuration, and associated data. This prevents unauthorized users from performing actions that may disable the TOE and result in undetected security events and issues.
O.COM_PROTECT	The TOE must make use of cryptographic functions for the protection of sensitive data in transit. Communication between the SmartConnectors and the ArcMC shall be protected using TLS. Communications between the TOE and trusted IT products (THUB) shall be protected using TLS. Communications between the TOE and web browsers shall be protected using HTTPS and TLS.

Table 8 – TOE Security Objectives

4.2. Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
OE.COM_PROTECT	The TOE operating environment must provide the cryptographic implementation that provides the protection of sensitive data in transit to and from the TOE. Web browsers used to access the TOE shall support HTTPS using TLS. External trusted IT products (THUB) shall support TLS.
OE.PERSONNEL	Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any administrator, user or operator of the TOE must be trusted to not disclose their authentication credentials. Authorized administrators are also required to manage and administer the TOE in a secure manner. Authorized administrators must be competent and security aware personnel in accordance with the administrator documentation.
OE.PHYSEC	The facility surrounding the TOE data must provide physical and logical controlled access.
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via OS).
OE.UPDATE	The TOE operational environment is updated by an administrator to address potential and actual vulnerabilities.

Table 9 – Operational Environment Security Objectives

4.3. Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVES / ASSUMPTIONS / THREATS / POLICIES	O.AUDIT	O.PRIVILEGE	O.SEC_ACCESS	O.COM_PROTECT	OE.COM_PROTECT	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC	OE.TIME	OE.UPDATE
A.AUDIT_PROTECT								✓		
A.HTTPS					✓					
A.LOCATE								✓		
A.MANAGE							✓			
A.NOEVIL							✓			
A.TIMESOURCE									✓	
A.UPDATE										✓
T.NO_AUTH	✓		✓			✓	✓	✓		
T.NO_PRIV	✓	✓	✓		✓					
T.SENSDATA			✓	✓	✓					

Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1. Mapping of Objectives:

ASSUMPTION / THREAT / POLICY	RATIONALE
A.AUDIT_PROTECT	This assumption is addressed by • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility.
A.HTTPS	This assumption is addressed by • OE.COM_PROTECT which ensures that Web browsers and web servers used to access the TOE shall support HTTPS using TLS.
A.LOCATE	This assumption is addressed by OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.MANAGE	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that the Authorized administrators are non-hostile and follow all administrator guidance.
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.
A.UPDATE	This assumption is addressed by OE. UPDATE. OE.UPDATE which requires the TOE operational environment be updated regularly to address potential and actual operational security issues.

ASSUMPTION / THREAT / POLICY	RATIONALE
T.NO_AUTH	This threat is countered by the following: • O.AUDIT, which ensures that all TOE transactions and attempted transactions are auditable and • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by competent and security aware personnel in accordance with the administrator documentation. As well as that any administrator, user, or operator of the TOE must be trusted to not disclose their authentication credentials. • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
T.NO_PRIV	This threat is countered by • O.AUDIT which ensures that all TOE transactions and attempted transactions are auditable • O.PRIVILEGE, which ensures that the TOE protects stored credentials from disclosure • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • OE_COM_PROTECT which ensures that sensitive data in transit is protected.
T.SENSDATA	This threat is countered by: • O.COM_PROTECT – which ensures the use of cryptographic functions provided by the operating environment to protect sensitive data in transit. • OE.COM_PROTECT – which ensures the use of cryptographic functions provided by the operating environment is used to protect communications with the TOE. • O.SEC_ACCESS which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications

Table 11– Mapping of Threats and Assumptions to Objectives

5. Extended Components Definition

There are no Extended Component requirements for the TOE.

6. Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1. Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in CC 2022 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by [*italicized text inside square brackets*].
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.
  When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

6.2. Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

FAU: Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.2	Protected Audit Data Storage
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.6	Timing and Event of Cryptographic Key Destruction
	FCS_RBG.1	Random Bit Generation (RBG)
	FCS_RBG.2	Random Bit Generation (external seeding)
	FCS_COP.1	Cryptographic Operation
FIA: Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
FPT: Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_STM.1	Reliable Time Stamps

	FPT_FLS.1	Fail Secure
	FPT_TST.1	TSF Self-test
FMT: Security Management	FMT_MOF.1	Management of Security Function Behaviour
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
FTA: TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
FTP: Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

Table 12 – TOE Security Functional Requirements

6.3. Security Audit (FAU)

6.3.1. FAU_GEN.1 Audit Data Generation

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 system;

b) All auditable events for the [*not specified*] level of audit; and

c) [The following Auditable events:
All use of the user identification mechanism
All use of the user authentication mechanism
Reaching the threshold for unsuccessful authentication attempts and actions taken by the TOE, including restoration to normal state (e.g. account unlocking)
All modifications to the behaviour of the security functions:
- create users
- query users
- delete users
- define network settings
- review audit logs

Modifications to the values of authentication data
Termination of an inactive session by the TSF
Termination of an inactive session by a user
].

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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information].

6.3.2. FAU_SAR.1 Audit Review

FAU_SAR.1.1 [Default System Admin, Read Only System Admin] with the capability to read [all ArcMC generated audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.3.3. FAU_SAR.2 Restricted Audit Review

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

6.3.4. FAU_SAR.3 Selectable Audit Review

FAU_SAR.3 The TSF shall provide the ability to apply [selection and ordering] of audit data based on [the following criteria:
• Selection based on date and time range and, optionally, subject identity and outcome
• Ordering based on date and time, subject identity, or type of event].

6.3.5. FAU_STG.2 Protected Audit Data Storage

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

6.4. Cryptographic Support (FCS) All provided by the environment

6.4.1. FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [See table below] and specified cryptographic key sizes [See table below] that meet the following: [See table below]

[

Key Generation Algorithm	Key Size	Standard	Algorithm Certificate
RSA	2048	FIPS 186-4	1985, A4270
AES GCM mode	128, 256 bits	FIPS 197	3895, A4270
SHA	256, 384	FIPS 180-4	3211, A4270

]

Application Note: This SFR corresponds to the correct invocation by the TOE, but not the implementation of cryptographic functionality.

6.4.2. FCS_CKM.3 Cryptographic Key Access (N/A)

FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].

Application Note: The TOE does not have key access. This is not applicable.

6.5. FCS_CKM.6 Timing and Event of Cryptographic Key Destruction

FCS_CKM.6.1 The TSF shall destroy [AES, RSA, ECDSA, SHA] when [*no longer needed*].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [no standard].

6.5.1. FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [Counter DRBG cert#C2204, Hash DRBG cert #1115] in accordance with [NIST SP800-90Ar1] after initialization with a seed.

FCS_RBG.1.2 The TSF shall use a [*TSF noise source]* [dev urandom]] for initialized seeding.

FCS_RBG.1.3 The TSF shall update the RBG state by [*reseeding, uninstantiating and re-instantiating*] using a [TSF noise source [dev urandom], ArcMC interface for seeding] in the following situations: [selection:

— on demand;

— on the condition: [module startup];

in accordance with [FIPS 140-2].

6.5.2. FCS_RBG.2 Random bit generation (external seeding)

FCS_RBG.2 The TSF shall be able to accept a minimum input of [128 bits] from a TSF interface for the purpose of seeding.

6.5.3. FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [self-test failure].

6.5.4. FPT_TST.1 TSF Self-Test

FPT_TST.1.1 The TSF shall run a suite of the following self-tests [*during initial start-up, at the request of the authorized use*] to demonstrate the correct operation of [*the TSF*]: [AES 256 Known Answer Test, RSA 2048 Pairwise Consistency Test, ECDSA

Pairwise Consistency Test, SHA256 and SHA384ntested with HMAC Known Answer Test, DRBG tests]

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF data*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF*].

6.6. FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [See table below] in accordance with a specified cryptographic algorithm [See table below] and cryptographic key sizes [See table below] that meet the following: [See table below].

[

Algorithm	Key Size	Standard	Algorithm Certificate
RSA	2048	FIPS 186-4	1985, A4270
AES GCM mode	128, 256	FIPS 197	3895, A4270
SHA	256, 384	FIPS 180-4	3211, A4270

]

6.7. Identification and authentication (FIA)

6.7.1. FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [Administrator configured] unsuccessful authentication attempts occur related to [user login].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [disable the user account for an administrator configurable period].

6.7.2. FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [username, password, permissions].

6.7.3. FIA_UAU.2 User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.7.4. FIA_UID.2 User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.8. Protection of the TSF (FPT)

6.8.1. FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

6.9. FPT_STM.1.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.10. Security Management (FMT)

6.10.1. FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify]* the functions [create users, query users, delete users, define network settings, and review audit logs] to [the authorized administrator].

6.10.2. Modify or delete FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*query, modify, delete*] the [user authentication data, configuration settings and audit logs] to [Administrator].

6.10.3. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:[

- create users
- query users
- delete users
- define network settings
- review audit logs].

6.10.4. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Default System Admin, Read Only System Admin, User].

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

6.11. TOE Access (FTA)

6.11.1. FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [Administrator-configurable period of inactivity.]

6.11.2. FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.12. Trusted Path / Channel

6.12.1. FTP_TRP.1 Trusted Path

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 [users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [administration, user access].

Note: The cryptography is provided by the environment.

6.12.2. FTP_ITC.1 Inter-TSF trusted channel

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, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [the establishment of TLS sessions].

6.13. Security Assurance Requirements

The assurance security requirements are summarized in the following table.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle Support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD	Developer defined life-cycle model
ASE: ST evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 13 – Security Assurance Requirements at EAL3+

6.14. Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access. The product was augmented to comply with ALC_FLR.3 in order to document and address requirements for remediation and reporting of faults that may be discovered in the product after release. The TOE invokes the environment cryptography to establish TLS 1.2 channels for secure communications.

6.15. Security Requirements Rationale

6.15.1. Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR CLAIM	DEPENDENCIES		DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1		YES	Satisfied by the Operational Environment
FAU_SAR.1	FAU_GEN.1		YES	
FAU_SAR.2	FAU_SAR.1		YES	
FAU_SAR.3	FAU_SAR.1		YES	
FAU_STG.2	FAU_GEN.1		YES	
FCS_CKM.1	FCS_COP.1 FCS_CKM.3 FCS_CKM.6 FCS_RBG.1	Yes N/A Yes Yes	YES	Provided by the environment
FCS_CKM.3	FCS_CKM.1	Yes		This is not required as the TOE does not access keys.
FCS_CKM.6	FCS_CKM.1	Yes	YES	Provided by the environment
FCS_RBG.1	FCS_RBG.2 FPT_FLS.1 FPT_TST.1	Yes Yes		Provided by the environment
FCS_RBG.2	FCS_RBG.1	Yes		Provided by the environment
FPT_FLS.1	None	N/A		Provided by the environment
FPT_TST.1	None	N/A		Provided by the environment

SFR CLAIM	DEPENDENCIES		DEPENDENCY MET	RATIONALE
FCS_COP.1	FCS_CKM.1, FCS_CKM.3	Yes N/A	YES	Provided by the environment
FIA_AFL.1	FIA_UAU.1			Since FIA_UAU.2 is hierarchical to FIA_UAU.1, this dependency is met.
FIA_ATD.1	None		N/A	
FIA_UAU.2	FIA_UID.1		YES	Since FIA_UID.2 is hierarchical to FIA_UID.1, this dependency is met.
FIA_UID.2	None		N/A	
FPT_ITT.1	None		N/A	
FPT_STM.1	None			Supplied by environment
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1		YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1		YES	
FMT_SMF.1	None		N/A	
FMT_SMR.1	FIA_UID.1		YES	Since FIA_UID.2 is hierarchical to FIA_UID.1, this dependency is met.
FPT_ITT.1	None		N/A	
FTA_SSL.3	None		N/A	
FTA_SSL.4	None		N/A	
FPT_ITC.1	N/A		N/A	
FTP_TRP.1	N/A		N/A	

Table 13 – Dependency Rationale

6.15.2. Security Functional Mappings

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.AUDIT	O.COM_PROTECT	O.PRIVILEGE	O.SEC_ACCESS
FAU_GEN.1	✓			
FAU_SAR.1	✓			
FAU_SAR.2	✓			
FAU_SAR.3	✓			
FAU_STG.2	✓			
FCS_CKM.1		✓		
FCS_CKM.3	Not applicable			
FCS_CKM.6		✓		
FCS_RBG.1		✓		
FCS_RBG.2		✓		
FPT_FLS.1		✓		
FPT_TST.1		✓		
FCS_COP.1		✓		
FIA_AFL.1			✓	✓
FIA_ATD.1			✓	✓
FIA_UAU.2			✓	✓
FIA_UID.2			✓	✓
FMT_MOF.1				✓
FMT_MTD.1				✓
FMT_SMF.1				✓
FMT_SMR.1				✓
FPT_ITT.1		✓		✓
FPT_STM.1	✓			
FTA_SSL.3				✓
FTA_SSL.4				✓
FTP_ITC.1		✓		
FTP_TRP.1		✓		

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

6.15.3. Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Objective	RATIONALE
O.AUDIT	This ensures that Audit events are logged and that the administrator can review these logs. • FAU_GEN.1 defines the auditing capability for events • FPT_STM.1 provides a reliable timestamp for audit entries • FAU_SAR.1 allows the review of the audited events • FAU_SAR.2 Restricts the audit review to the administrator • FAU_SAR.3 Allows the administrator to view the audit logs selectively. • FAU_STG.2 ensures audit data cannot be modified.
O.COM_PROTECT	This objective ensures that sensitive data in transit is protected[1]. The objective also ensures the confidentiality of data passed between itself and remote users, and between the TOE and external web servers. • FPT_ITC.1 specifies communications between the TOE and trusted IT products is protected. • FTP_TRP.1 specifies that the TSF provides a distinct trusted communication path to/from TOE. • FPT_ITT.1 provides a trusted channel between ArcMC and the SmartConnectors. • FCS_CKM.1, FCS_CKM.6, FCS_RBG.1, FCS_RBG.2, FPT_FLS.1, FPT_TST.1 and FCS_COP.1 are all met by the environment but provide the encryption for the TOE. • FCS_CKM.1 and FCS_COP.1 specify the keys that are generated and used. • FCS_CKM.6 specifies the destruction of the keys when no longer needed. • FCS_RBG.1 specifies the random number generator that creates the keys. • FCS_RBG.2 specifies the entropy for the RBG. • FPT_FLS.1 ensures a failure to secure mode when an error occurs. • FPT_TST.1 runs self-tests to ensure correct operation. • **Note:** FCS_CKM.3 is not applicable as the TOE has no access to keys.
O.SEC_ACCESS	This objective ensures that the TOE shall ensure that only Administrators, System Users, and authorized users and applications are granted access to security functions, configuration, and associated data only by authorized users and applications. • FIA_AFL.1 ensures only authorized personnel can access the TOE • FIA_ATD.1 specifies security attributes for users of the TOE • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to configuration of the TOE • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE

[1] Note encryption is provided by the operating environment.

Objective	RATIONALE
	• that will override default values. • FMT_MTD.1 restricts the ability to perform the functions on TSF data listed in in the SFR to the Administrator. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role. • FTA_SSL.3 requires the TSF terminate an interactive session after an administrator configured period. • FTA_SSL.4 requires the user be able to terminate their own session. • FPT_ITT.1 provides a trusted channel between ArcMC and the SmartConnectors. • FMT_MOF.1 ensures that the management of the TOE is restricted to authorized administrators.
O.PRIVILEGE	This objective ensures that all stored credentials are protected from disclosure. • FIA_AFL.1 ensures only authorized personnel can access the TOE. • FIA_ATD.1 specifies security attributes for users of the TOE. • FIA_UID.2 requires a user to be identified before any interaction with the TOE can occur • FIA_UAU.2 requires a user to be authenticated before any interaction with the TOE can occur

Table 16 – Rationale for TOE

7. TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1. TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path

7.2. Security Audit

The TOE audits events. The Administrator is able to view and sort these logs. The timestamp is provided by the OS.The table below describes the Security Audit functions along with their SFRs.

Functional Description	SFR
The TOE generates the following audit data: Start-up and shutdown of the audit functions (instantiated by start-up of the TOE) User login/logout, Login failures All User access and activities performed while accessing systems] The TOE records the date, time and type of event as well as the subject identity and outcome of the event. A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date are provided by the operational environment. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.	FAU_GEN.1 FPT_STM.1
The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console or via the external event sources. The Console provides a suitable means for the Administrator to interpret the information from the audit log. Audit records can be searched using filters.	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3
The audit trail is protected from deletion and disclosure.	FAU_STG.1

7.3. Cryptographic Support

The TOE relies on the environment to provide the cryptography for TLS v1.2 protected communications. Voltage provides algorithms for format preserving encryption. The following table states what cryptographic algorithms are being used:

Key Generation Algorithm	Key Size	Standard	Certificate
RSA	2048	FIPS 186-4	1985, C2204
ECDSA	Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	FIPS 186-4	846, C2204
AES GCM mode	128, 192, 256 bits	FIPS 197	3895, C2204
AES CBC mode	128, 192, 256 bits	FIPS 197	3895

SHA	256, 384	FIPS 180-4	3211, C2204

The table below describes the Cryptographic Support provided by the environment along with their SFRs.

Functional Description	SFR
Keys are generated by Voltage using a HASH DRBG. Keys are generated by Bouncy Castle using a Counter DRBG.	FCS_CKM.1
The TOE has no access to keys so this SFR is not applicable.	FCS_CKM.3
The Toe destroys keys that are used once they are no longer required.	FCS_CKM.6
A DRBG is used to generate keys.	FCS_RBG.1
The entropy source for the DRBGs is dev urandom.	FCS_RBG.2
The cryptomodule fails securely if a self-test fails.	FPT_FLS.1
The cryptomodule runs self-tests including an integrity test of the entire module at startup and on demand. These self-tests ensure the cryptographic algorithms used are operating properly.	FPT_TST.1
The cryptographic algorithms are used to establish TLS connections. Voltage is used to produce format preserving encryption.	FCS_COP.1

7.4. Identification and Authentication

Identification and Authentication of all users is required in order to access to TOE. The table below describes the Identification functions along with their SFRs.

Functional Description	SFR
The number of login incorrect login attempts that occur is configurable by the Administrator. In tis evaluation the number incorrect logins is 3.When this has been reached, the user account is disabled.	FIA_AFL.1
The TOE maintains the following list of security attributes belonging to individual users: • User Identity (i.e., username) • Password • permissions	FIA_ATD.1
The TOE enforces individual authentication and provides a centralized authentication mechanism. Administrators and Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE.	FIA_UAU.2
The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Administrators and Users with management access must successfully identify themselves using a unique identifier and authenticator prior to performing any actions on the TOE.	FIA_UID.2

7.5. Security Management

Security Management is provided by enforcing roles and rules. Each role consists of a series of privileges. Roles can have privileges added to or removed from them. These roles are then

assigned to individuals. In addition, rules can be specified controlling where and when the privileges may be used. Note a user may only have one role at a time.
The table below describes the TOE management functions along with their SFRs.

Functional Description	SFR
Only the Administrator can control user privileges and user accounts attributes.	FMT_MTD.1, FMT_MOF.1
The TOE supports the following management functions: create users query users delete users define network settings review audit logs	FMT_SMF.1
The TOE provides Administrator, User, and user roles. Administrator functions are defined in FMT_SMF.1. User privileges may only be modified by an authorized Administrator.	FMT_SMR.1

Table 4 – Security Management Functions and SFRs

7.6. Protection of the TSF

The TOE protects data transfers between TOE components using environmentally provided cryptography and HTTPS/TLS.

- FPT_ITT.1

7.7. TOE Access

The TOE can terminate sessions either via a pre-configured inactivity timeout or via a user-initiated timeout. The TOE can also prevent TOE users (Administrators, Users), from accessing the system outside of their authorized time.

Functional Description	SFR
The TOE provides the capability for TSF initiated termination of an interactive session after an administrator configurable period of inactivity.	FTA_SSL.3
The TOE provides the TSF with the ability to allow users to initiate termination of their interactive session.	FTA_SSL.4

Table 18 – TOE Access

7.8. Trusted Path

The Environment provides the cryptographic algorithms needed to establish a trusted path using TLS v1.2. The table below describes the TOE management functions along with their SFRs.

Functional Description	SFR
The TOE OE provides the trusted path for TOE Users, using environmentally provided cryptography for HTTPS/TLS.	FTP_TRP.1
The TOE OE provides a trusted channel between the parts or the TOE (ArcMC and SmartConnectors)	FTP_ITC.1

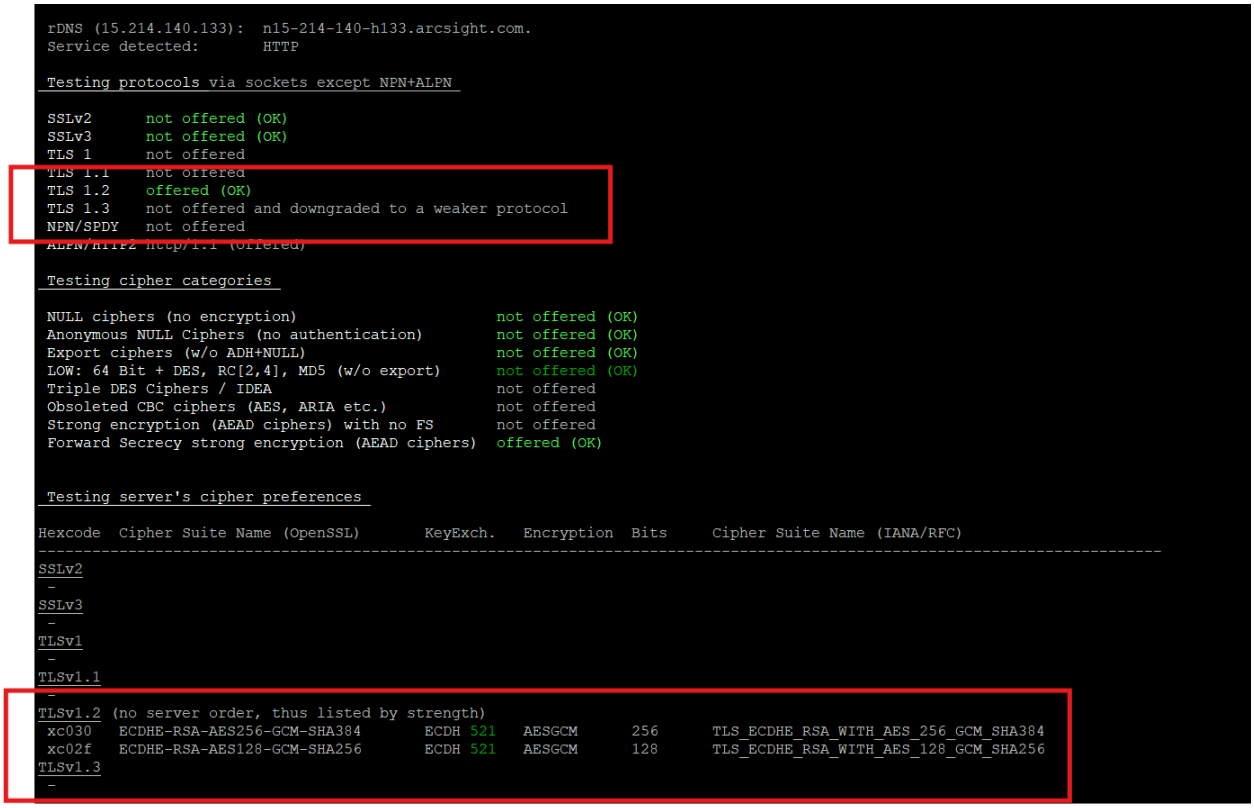
The Environment provides Bouncy Castle version 2.1.0 (CMVP certificate # 4943) to protect communications between ArcMC and the SmartConnectors.

The environment provides TLS v1.2 to protect communications between the Browser and the ArcMC.

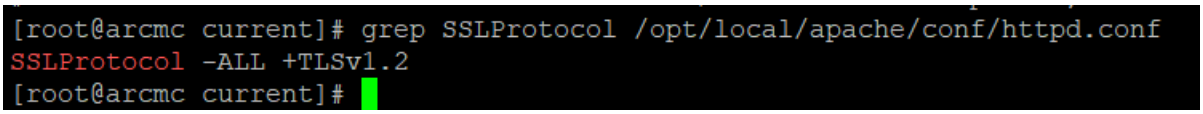
Using the environment provided Voltage Cryptographic Module v5.0 (CMVP certificate #2686). The TOE OE supports TLS v1.2.

The cipher suites used by ArcMC are:

ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-GCM-SHA256



Version of TLS for ArcMC



The cipher suite used by the SmartConnectors is:
ECDHE-RSA-AES-128-GCM-SHA256

```
 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order)
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 521   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLSv1.3
 -
```

Version of TLS for SmartConnectors

```
[root@arcmc current]# grep -i TLSv ./config/agent/agent.defaults.properties
remote.management.ssl.enabled.protocols=TLSv1.2
remote.management.ssl.fips.enabled.protocols=TLSv1.2
ssl.protocols=TLSv1.2
```