# CA Technologies

## CA API Gateway v9.2

# Security Target

**September 2017**


**Document prepared by**


Ark Infosec Labs Inc.
www.arkinfosec.net

# Document History

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 17 Aug 2017 | L Turner | Final for certification. |
| 1.1 | 21 Sep 2017 | L Turner | Update CMVP certificate for HSM. |

# Table of Contents



# List of Tables

# List of Figures

# 1 Introduction

## 1.1 Overview

1 The CA API Gateway is an enterprise security management solution that provides centralized management and access control over web services and related resources. The Gateway is designed to protect web services and mediate communications between Service Oriented Architecture (SOA) clients and endpoints residing in different identity, security, or middleware domains.

2 This Security Target (ST) defines the CA API Gateway v9.2 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

3 For a precise statement of the scope of incorporated security features, refer to section 2.3.

## 1.2 Identification

**Table 1: Evaluation identifiers**

| | |
|---|---|
| **Target of Evaluation** | CA Technologies CA API Gateway v9.2<br>Build: 6904<br>Patch: CA_API_nShieldUpdate_64bit_v12.30.00.L7P |
| **Security Target** | CA Technologies CA API Gateway v9.2 Security Target, v1.1 |

## 1.3 Conformance Claims

4 This ST supports the following conformance claims:

a) CC version 3.1 Revision 4, September 2012

b) CC Part 2 extended

c) CC Part 3 conformant

d) Exact conformance to:

i) Standard Protection Profile for Enterprise Security Management Policy Management, v2.1, 24 October 2013 (ESM Policy Manager PP)

ii) Standard Protection Profile for Enterprise Security Management Access Control, v2.1, 24 October 2013 (ESM Access Control PP) – Architectural Variation: Web Based Access Control

e) Related Technical Decisions:

i) TD0042: Removal of Low-level Crypto Failure Audit from PPs

ii) TD0055: Move FTA_TAB.1 to Selection-Based Requirement

iii) TD0066: Clarification of FAU_STG_EXT.1 Requirement in ESM PPs

iv) TD0071: Use of SHA-512 in ESM PPs

v) TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1

## 1.4 Terminology

**Table 2: Terminology**

| Term | Definition |
|---|---|
| API | Application Programming Interface |
| CA | Certificate Authority |
| CC | Common Criteria |
| DMZ | Demilitarized Zone |
| EAL | Evaluation Assurance Level |
| ESM | Enterprise Security Management |
| FTP | File Transfer Protocol |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| ICAP | Internet Content Adaptation Protocol |
| Identity Provider | A user database (internal or external) within the context of the TOE. |
| JDBC | Java Database Connectivity |
| JMS | Java Message Service |
| LDAP | Lightweight Directory Access Protocol |
| MQ Native | Refers to MQ Native Queues that can be used by the CA Gateway to natively communicate with IBM WebSphere MQ message-oriented middleware. |
| NTP | Network Time Protocol |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| SOA | Service Oriented Architecture |
| SOAP | Simple Object Access Protocol. SOAP defines the message format used in web services requests. |
| SSH | Secure Shell |
| ST | Security Target |

| Term | Definition |
|---|---|
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TSF | TOE Security Functions |
| TOE | Target of Evaluation |
| UDDI | Universal Description, Discovery and Integration |
| URL | Universal Resource Locator |
| WSDL | Web Services Description Language |
| WS-Security | WS-Security (Web Services Security) is an extension to SOAP to apply security to web services. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. |
| XML | Extensible Markup Language |
| XSL | Extensible Stylesheet Language |

# 2 TOE Description

## 2.1 Type and Usage

5 The TOE is an enterprise security management solution that provides centralized management and access control over SOAP web services. The TOE controls how SOAP web services are exposed to and accessed by external client applications.

6 As shown in Figure 1, the TOE is comprised of two main components for policy definition and policy consumption:

a) **Policy Manager.** A GUI application that provides the user with the primary administrative interface to the Gateway. The Policy Manager is used to construct policies and administer the TOE.

b) **Gateway.** One or more hardware or virtual appliances that enforce policy assertions to control web services. Basic configuration is performed using the Gateway Configuration Utility – a menu based Command Line Interface (CLI). The Gateway consumes policies defined by the Policy Manager which also provides the primary administrative interface.

7 The Gateway interfaces with client-side applications that require communication with web services. Client systems send message requests intended for the web service to the Gateway. The Gateway then functions as a client-side proxy, enforcing access control decisions and applying necessary requirements such as identities, protocols, headers, and/or transformations to the message as required by the policy in use. Policies modified through the Policy Manager are automatically applied in real time by the Gateway to ensure that all subsequent messages conform to the updated policy.

8 In a typical network, the Gateway resides in the demilitarized zone (DMZ), shielding downstream services as it enforces policy assertions on incoming and outgoing messages. A typical TOE deployment is depicted in Figure 1.

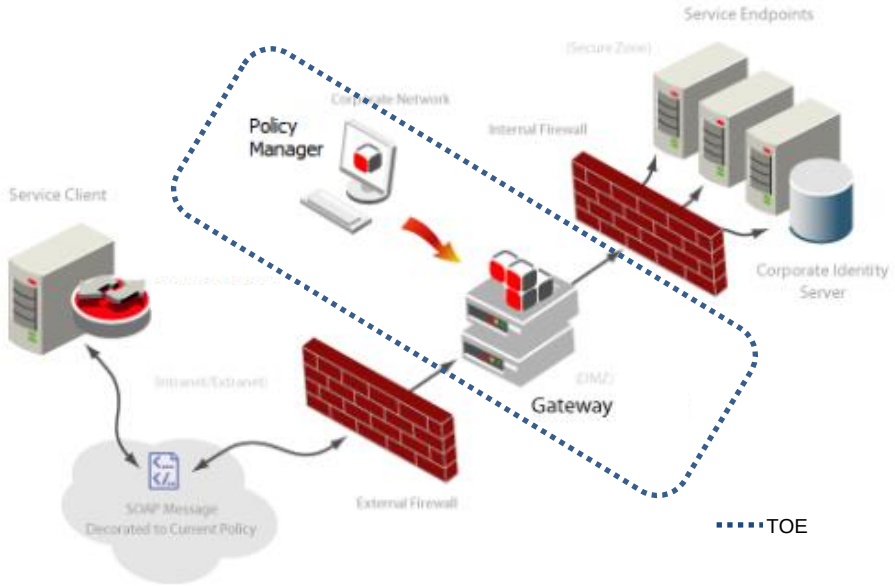


**Figure 1: TOE deployment scenario**

9 Figure 1 shows the following non-TOE components:

a) **Service client.** An external IT entity that accesses web services via the Gateway. Service clients do not log into the TOE.

b) **Firewalls.** Corporate firewalls providing traditional perimeter security.

c) **Service endpoints.** An enterprise IT entity that provides SOAP web services via the Gateway.

d) **Corporate identity server.** An enterprise IT entity that provides identity services – such as an LDAP directory.

## 2.2 Architecture

10 Endpoints and clients that communicate via the Gateway are Hypertext Transfer Protocol (HTTP), Java Message Service (JMS), File Transfer Protocol (FTP) or raw Transmission Control Protocol (TCP) socket accessible applications. Clients access the Gateway via a Universal Resource Locator (URL) queue or socket that is compatible with one of the above protocols. The Gateway functions as a reverse proxy for service requests and should be the single web service traffic enforcement point in a network.

11 Figure 2 below illustrates the architectural layers and deployment options of the Gateway component of the TOE –Standalone Gateway (dark blue), Basic Cluster Gateway (yellow), Extended Gateway Cluster (green excluding the load balancer), Each layer in Figure 2 below is described in the following sections. Figure 2 uses the abbreviation SSG to refer to the CA API Gateway. Figure 2 is not intended to illustrate TOE scope (refer to sections 2.5 and 2.6). The Policy Manager is not shown.

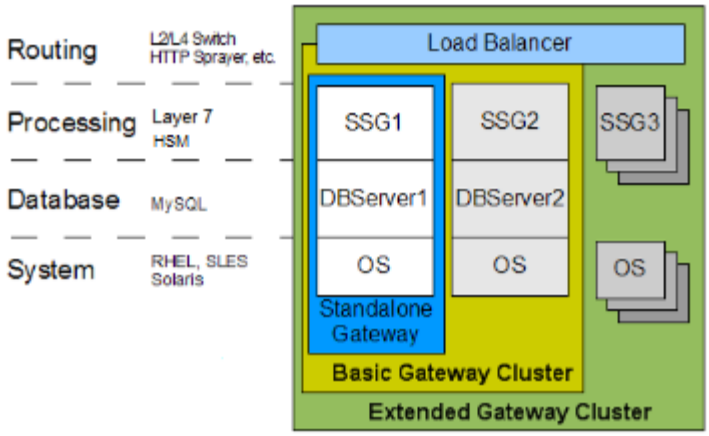


**Figure 2: Gateway architecture**

### 2.2.1 Routing Layer

12 External to the TOE, the Routing Layer represents an industry-standard load balancer configured to provide TCP-level load balancing and failover. It is not required for a standalone Gateway.

### 2.2.2 Processing Layer

13 The Processing Layer represents the Gateway's core runtime component. When a request message is received, the Gateway executes a service resolution process that attempts to identify the targeted destination service. When a published service is resolved, the Gateway executes the Policy Manager-configured policy for the service. If the policy assertions succeed, then the request is routed; if one or more policy assertions fail, then the request is either denied with a SOAP fault or the connection is dropped. In a Gateway cluster, systems that are installed with this runtime component are referred to as "Processing Nodes".

14 The Processing Layer may also involve the following components:

a) **Identity providers.** The Gateway uses identity providers to authenticate and identify users and groups when authenticating messages and administrative access. The Gateway can use its built-in identity provider (called the Internal Identity Provider or the Federated Identity Provider in an identity bridging scenario) or interface directly with any LDAP-based identity provider.

b) **Trust store.** The Gateway maintains a trust store of certificates that do not belong to it but that are trusted and used for one or more vital security functions, such as signing client certificates. Certificates are imported into the Gateway trust store via the Policy Manager. The Gateway can be configured to perform revocation checking for certificates through Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

c) **UDDI.** The Gateway supports publishing of web services by using the Web Services Description Language (WSDL) located in a Universal Description, Discovery and Integration (UDDI) registry. **Note:** UDDI is not supported in the evaluated configuration.

d) **Logging and auditing functionality.** The Gateway provides several logging and auditing features, allowing users to monitor the activity and health of the Gateway, and the ongoing success or failure of service policy resolution. Auditing is provided for all system events, and is configurable for individual service policies. All audit records can be viewed through the Policy Manager. Gateway logging is performed during runtime, and those logs can also be viewed through the Policy Manager. The Manager also features a Dashboard that allows administrators to monitor activity through the Gateway in real-time.

### 2.2.3 Database Layer

15 The Gateway stores policies, processing audits, Internal Identity Provider, keystore, configuration details and other information in a MySQL database. In a typical configuration this database will reside on the same physical system as a Processing Node, although in rare circumstances it may reside on a separate system.

16 In a Gateway cluster, systems that are installed with the database component are referred to as "Database Nodes". There will typically be two replicated Database Nodes in a cluster: Primary and Secondary. The Processing Nodes are configured to communicate with one of the Database Nodes (normally the Primary) and then fail over to the Secondary Database Node should the Primary become unavailable.

### 2.2.4 System Layer

17 The System Layer represents the Operating System (Red Hat Enterprise Linux), Java Virtual Machine (Sun JDK) and hardware / virtual platform.

## 2.3 Evaluated Configuration

18 The following sections describe the high-level configuration of the TOE. Assurance gained from evaluation is only applicable to the configurations and components that are identified within. Detailed guidance for establishing the evaluated configuration is provided in the *CA Technologies CA API Gateway* v9.2 *Secure Installation Guide*.

19 Refer to section 2.5 below for details of the hardware and software that is included in the evaluated configuration.

### 2.3.1 Architecture

20 The evaluated configuration of the TOE reflects the following architectural decisions:

a) **Routing Layer.** The presence of a load balancer is determined by whether the TOE is deployed in a standalone or cluster configuration. Only standalone Gateway deployments are included in the evaluated configuration. The load balancer is not part of the TOE.

b) **Processing Layer**

i) **Identity providers.** The evaluated configuration supports the Internal Identity Provider and Federated Identity Providers with an X.509 credential source. Federated Identity Providers with SAML credential source and custom identity assertions are excluded from the evaluated configuration. The Internal Identity Provider is part of the TOE, Federated Identity Providers require an identity server to be present in the environment. In the evaluated configuration, TOE administrative users may only authenticate against LDAP-based identity providers.

ii) **Trust store.** The Gateway is configured to perform revocation checking for certificates using either CRL or OCSP. The trust store is part of the TOE.

iii) **UDDI**. UDDI functionality is not within the scope of the TOE.

iv) **Logging and auditing.** The evaluated configuration includes logging to the internal database and/or an external Syslog server. The internal database is part of the TOE.

v) **Hardware Security Module (HSM)** Hardware module for cryptographic operations. See section 2.3.2 below. HSMs are not part of the TOE but must be used if deploying the hardware Gateway Appliance.

c) **Database Layer.** The MySQL database may reside on a Processing Node or Database node. The database is part of the TOE.

d) **System Layer.** In the evaluated configuration, the Gateway component of the TOE may be deployed on a hardware or virtual appliance however the virtualization server platform is not part of the TOE.

### 2.3.2 Keystore & Cryptographic Operations

21 The TOE requires a keystore which is implemented internally unless a HSM is present as described below. The TOE provides its own internal cryptographic functionality for SSH connections (remote administration) but relies on third party software or hardware modules to perform all other cryptographic operations for the TOE as follows:

i) **Gateway software cryptographic module.** Cryptographic operations of the soft appliance are provided by CryptoComply CCJ 1.0 (CMVP

Certificate No. 2483). CA affirms that the module has not been altered and operates correctly on the TOE java runtime environment.

ii) **Gateway hardware cryptographic module.** Keystore and cryptographic operations of the hardware Gateway Appliance are provided by the Thales nShield HSM[1] (CMVP Certificate No. 2638).

iii) **Policy manager software cryptographic module.** Policy manager cryptographic operations are provided by CryptoComply CCJ 1.0 (CMVP Certificate No. 2483). CA affirms that the module has not been altered and operates correctly on the TOE java runtime environment.

22 The evaluated configuration assumes that the TOE is configured to be in FIPS mode (*security.fips.enabled* – refer to *Miscellaneous Cluster Properties* in the *Online Documentation*).

### 2.3.3 Management

23 The Gateway can be managed in by a number of different interfaces / applications. Only the Policy Manager application and Gateway Configuration Utility are included in the evaluated configuration.

24 The Policy Manager web interface and Enterprise Security Manager application are excluded from the evaluated configuration.

## 2.4 Security Functions

25 The following sections describe the security functions provided by the TOE (refer to section 6 for additional detail on each security function).

### 2.4.1 Access Control Policy Definition

26 The Policy Manager allows the TOE administrator to define detailed policies to enforce robust access control over web services. The following policy assertions are covered by the evaluation:

a) **Access control assertions.** The following subset of access control assertions are evaluated:

i) **Authenticate User or Group.** Require specified users and/or groups to be authenticated against a selected identity provider. Applies the credentials collected by a 'require' assertion listed below to authenticate a user or group specified in this 'authenticate' assertion.

ii) **Authenticate against Identity Provider.** Requires provided client credentials to be successfully authenticated against a selected identity provider. Applies the credentials collected by the 'require' assertions to be authenticated.

iii) **Require HTTP Basic** (**Note:** should be used in conjunction with Require SSL or TLS). Require that incoming requests to contain HTTP basic authentication credentials.

iv) **Require SAML Token Profile.** Requires incoming requests to contain a SAML (Security Assertions Markup Language) token. **Note:** The

[1] Evaluation test platform configured with the nShield F3 6000+ (Model: nC4433E-6K0). Security Policy: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2638.pdf

evaluated configuration defined in the *Secure Installation Guide* specifies a limited set of SAML attributes that may be used.

v) **Require SSL or TLS Transport with Client Authentication.** Requires clients to connect via SSL or TLS and optionally to provide a valid / trusted X.509 certificate.
**Note:** This assertion appears in two different assertion palettes:

- When accessed from the Access Control palette, this assertion is labeled "Require SSL or TLS Transport with Client Authentication" and has the Require Client Certificate Authentication check box selected by default.
- When accessed from the Transport Layer Security palette, this assertion is labeled "Require SSL or TLS Transport" and does not have the Require Client Certificate Authentication check box selected by default.

vi) **Require WS-Security Signature Credentials.** Requires that the web service target message includes an X.509 client certificate and has at least one element signed by that client certificate's private key as a proof of possession.
**Note:** The evaluated configuration defined in the *Secure Installation Guide* specifies a limited set of attributes that may be used with this assertion – multiple signatures are not supported.

b) **Service availability assertions.** The following subset of service availability assertions are evaluated:

i) **Limit Availability to Time/Days.** Enables restricting service access by a time and/or day interval. When the Gateway receives a request for the service, it will check the time and/or day restrictions before allowing the message to proceed.

ii) **Restrict Access to IP Address Range.** Enables restricting service access based on the IP address of the requesting service client.

c) **Policy logic assertions.** The following subset of policy logic assertions are evaluated in support of access control:

i) **All Assertions Must Evaluate to True.** All associated assertions must evaluate to true to achieve a ‘success outcome’.

ii) **At Least One Assertion Must Evaluate to True.** At least one associated assertion must evaluate to true to achieve a ‘success outcome’.

27 The Policy Manager can detect inconsistencies in the application of policies so that policies are unambiguously defined.

28 The Policy Manager uniquely identifies the policies it creates so that it can be used to determine what policies are being implemented by remote products.

### 2.4.2 Access Control Policy Enforcement

29 The Gateway enforces the policies defined by the Policy Manager. The Gateway inspects messages sent between service clients (request messages) and service endpoints (response messages) to evaluate and enforce compliance with the defined policies.

### 2.4.3 Policy Security

30 Communication between the Policy Manager and the Gateway is protected from disclosure and modification. A trusted channel is established to identify and authenticate each end point using TLS client / server authentication.

31 The Gateway validates the integrity of the policy data it receives and rejects any invalid or replayed data. The Gateway generates evidence of receipt of policies.

32 The TOE protects the integrity of policy, identity, credential, attribute, and other security information obtained from other trusted IT entities.

### 2.4.4 System Monitoring

33 The TOE provides the ability to keep an audit/log trail to provide administrative insight into system management and operation, including identifying what policies are being defined and enforced. The TOE is capable of sending audit/log information to an external trusted entity.

34 The following policy assertions are used in support of system monitoring:

a) **Audit Message in Policy.** Enables auditing of messages within a policy. It records events pertaining to the processing of a policy— e.g. assertion violations.

b) **Add Audit Detail.** Allows the definition of a custom message that can enhance the context of an audit message.

c) **Customize SOAP Fault Response.** Allows customization of the SOAP fault response on a policy-by-policy basis.

### 2.4.5 Secure Administration

35 Administrative access to the TOE requires authentication and is governed by role based access control. The TOE protects against attacker attempts to illicitly authenticate using repeated guesses and enforces an administrator define password policy. The TOE displays a banner at login. Remote access to the Gateway Configuration CLI is protected via SSH and the underlying cryptography for SSH is provided by the Gateway's OS.

### 2.4.6 Continuity of Enforcement

36 The Gateway will continue policy enforcement in the event of a loss of connectivity with the Policy Manager.

## 2.5 Physical Scope

37 The TOE, in the evaluated configuration, consists of the following components:

a) **Policy Manager.** The application software running on non-TOE operating system (Windows 7).

b) **Gateway.** The CA API Gateway in one of the following form factors:

i) **CA Technologies CA API Gateway Appliance.** Gateway ships on hardware and configured to use the Thales nShield HSM (sold separately – see section 2.3.2). This includes:

**(1)** Oracle X5-2 Server

**(2)** Red Hat Enterprise Linux (RHEL) Server v6.8

ii) **CA Technologies CA API Gateway Soft Appliance.** Gateway ships as a virtual appliance.

### 2.5.1 Guidance Documents

38 The TOE includes the following guidance:

a) CA Technologies CA API Gateway v9.2 Online Documentation (available at https://docops.ca.com/ca-api-gateway/9-2/en)

b) CA Technologies CA API Gateway v9.2 Secure Installation Guide

### 2.5.2 Non-TOE Components

39 The Gateway Soft Appliance requires the following:

a) **Virtualization Server.** VMWare vSphere v5.5.0.

40 **Note:** Other Virtualization Servers are supported however are excluded from the scope of evaluation.

41 The Policy Manager application requires the following:

a) Microsoft Windows 7

b) Java Virtual Machine: JRE 8u102

42 **Note:** Other Operating Systems are supported however are excluded from the scope of evaluation.

43 The TOE operates with the following components in the environment:

a) **Audit server.** The TOE utilizes a Syslog server to store audit records.

b) **Time server.** The TOE utilizes a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.

c) **Identity server.** An LDAP 3.0 directory server is required for the Policy Manager user database. Microsoft Active Directory is specified for the evaluated configuration.

d) **Hardware Security Module.** In the evaluated configuration, the Gateway Appliance must be configured to use the Thales nShield HSM for the keystore & cryptographic operations. Refer to section 2.3.2 for details. **Note:** This only applies to the hardware appliance, not the soft (virtual) appliance.

## 2.6 Logical Scope

### 2.6.1 Evaluated Features

44 The logical scope of the TOE comprises the security functions defined in section 2.4 based on the evaluated configuration specified in section 2.3.

45 Administrators should configure the TOE according to the *CA Technologies CA API Gateway* v9.2 *Secure Installation Guide* to establish the Common Criteria evaluated configuration.

### 2.6.2 Unevaluated Features

46 The following security related features have not been evaluated:

a) Gateway Appliance Firewall (IP Tables)

b) UDDI Registries

c) Policy Manager Audit Alerts

d) Security Zones

e) SFTP Polling Listeners

f) Working with SiteMinder

g) Use the Gateway as an HTTP Proxy

h) Salesforce Integration

i) Windows Domain Login

j) Gateway Backup and Restore

k) Gateway Patch Management

l) Mediation of access to non-SOAP web services

m) Authentication performed by Federated Identity Providers – the evaluation ensures that the result of the authentication is enforced but does not evaluate the authentication itself as this is performed by a third party providers. In addition, the evaluated configuration does not include use of the following Identity Providers:

   i) Federated Identity Provider using SAML credential source

n) Global Policy Fragments

### 2.6.3 Scope of Evaluated Policy Assertions

47 The core functionality of the CA API Gateway is its ability to define and enforce policies for web services. To achieve this, the CA API Gateway utilizes a policy assertion language. All available policy assertions are defined in the *Assertion Palette* section of the *Online Documentation.* Not all policies are related to access control or security – in order to clarify the relationship between policy assertions and the scope of evaluation, the following table classifies each policy assertion as one of the following:

a) **Enforcing.** Assertions that enforce the TOE security policy and are the focus of this evaluation.

b) **Unevaluated Functional.** Assertions that facilitate product functionality and may be present in the evaluated configuration but that do not interfere with the security functions of the TOE. Such assertions have not been evaluated.

c) **Unevaluated Security.** Assertions that are security related but have not been evaluated.

**Table 3: Scope of evaluated policy assertions**

| **Assertion** | **Enforcing** | **Unevaluated Functional** | **Unevaluated Security** |
|---|---|---|---|
| **Access Control Assertions** | | | |
| Authenticate User or Group Assertion | X | | |

| Assertion | Enforcing | Unevaluated Functional | Unevaluated Security |
|---|---|---|---|
| Authenticate Against Identity Provider Assertion | X | | |
| Require HTTP Basic Credentials Assertion | X | | |
| Require SAML Token Profile Assertion | X | | |
| Require SSL or TLS Transport Assertion with Client Authentication (same as Transport Layer Security assertion: Require SSL or TLS Transport Assertion) | X | | |
| Authenticate Against SiteMinder Assertion | | | X |
| Authorize via SiteMinder Assertion | | | X |
| Check Protected Resource Against SiteMinder Assertion | | | X |
| Exchange Credentials using WS-Trust Assertion | | | X |
| Extract Attributes from Certificate Assertion | | | X |
| Extract Attributes for Authenticated User Assertion | | | X |
| Perform JDBC Query Assertion | | | X |
| Query LDAP Assertion | | | X |
| Require Encrypted Username Token Profile Credentials Assertion | | | X |
| Require FTP Credentials Assertion | | | X |
| Require HTTP Cookie Assertion | | | X |
| Require Remote Domain Identity Assertion | | | X |
| Require NTLM Authentication Credentials Assertion | | | X |
| Require SSH Credentials Assertion | | | X |
| Require Windows Integrated Authentication Credentials Assertion | | | X |
| Require WS-Secure Conversation Assertion | | | X |
| Require WS-Security Kerberos Token Profile Credentials Assertion | | | X |
| Require WS-Security Password Digest Credentials Assertion | | | X |

| Assertion | Enforcing | Unevaluated Functional | Unevaluated Security |
|---|---|---|---|
| Require WS-Security Signature Credentials Assertion | X | | |
| Require WS-Security UsernameToken Profile Credentials Assertion | | | X |
| Require XPath Credentials Assertion | | | X |
| Retrieve Credentials from Context Variable Assertion | | | X |
| Retrieve Kerberos Authentication Credentials Assertion | | | X |
| Retrieve SAML Browser Artifact Assertion | | | X |
| Use WS-Federation Credential Assertion | | | X |
| **Transport Layer Security Assertions** | | | |
| Require SSL or TLS Transport (same as Access Control assertion: Require SSL or TLS Transport Assertion with Client Authentication) | X | | |
| **XML Security Assertions** | | | X |
| **Message Validation / Transformation Assertions** | | X | |
| **Message Routing Assertions** | | | |
| Add Header Assertion | | X | |
| Configure Message Streaming Assertion | | X | |
| Copy Request Message to Response Assertion | | X | |
| Execute Salesforce Operation | | X | |
| Return Template Response to Requestor Assertion | | X | |
| Route via FTP(S) Assertion – Configured with FTP | | X | |
| Route via FTP(S) Assertion – Configured with FTPS | | | X |
| Route via HTTP(S) Assertion – Configured with HTTP | | X | |
| Route via HTTP(S) Assertion – Configured with HTTPS | | | X |
| Route via JMS Assertion | | X | |
| Route via MQ Native Assertion | | X | |

| Assertion | Enforcing | Unevaluated Functional | Unevaluated Security |
|---|---|---|---|
| Route via Raw TCP Assertion | | X | |
| Route via SecureSpan Bridge Assertion | | | X |
| Route via SSH2 Assertion | | | X |
| **Service Availability Assertions** | | | |
| Limit Availability to Time/Days Assertion | X | | |
| Restrict Access to IP Address Range Assertion | X | | |
| Apply Rate Limit Assertion | | X | |
| Apply Throughput Quota Assertion | | X | |
| Look Up in Cache Assertion | | X | |
| Query Rate Limit Assertion | | X | |
| Query Throughput Quota Assertion | | X | |
| Resolve Service Assertion | | X | |
| Store to Cache Assertion | | X | |
| **Logging, Auditing, and Alerts Assertions** | | | |
| Add Audit Detail Assertion | X | | |
| Audit Messages in Policy Assertion | X | | |
| Capture Identity of Requestor Assertion | | X | |
| Customize Error Response Assertion | | X | |
| Customize SOAP Fault Response Assertion | X | | |
| Send Email Alert Assertion | | | X |
| Send SNMP Trap Assertion | | X | |
| **Policy Logic Assertions** | | | |
| Add Comment to Policy Assertion | | X | |

| Assertion | Enforcing | Unevaluated Functional | Unevaluated Security |
|---|---|---|---|
| All Assertions Must Evaluate to True Assertion | X | | |
| At Least One Assertion Must Evaluate to True Assertion | X | | |
| Compare Expression Assertion | | | X |
| Continue Processing Assertion | | | X |
| Create Routing Strategy Assertion | | | X |
| Execute Routing Strategy Assertion | | | X |
| Export Variables from Fragment Assertion | | | X |
| Generate UUID Assertion | | | X |
| Include Policy Fragment Assertion | | | X |
| Join Variable Assertion | | | X |
| Look Up Context Variable | | | X |
| Look Up Item by Value Assertion | | | X |
| Look Up Item by Index Position Assertion | | | X |
| Manipulate Multivalued Variable Assertion | | | X |
| Map Value Assertion | | | X |
| Process Routing Strategy Result Assertion | | | X |
| Run All Assertions Concurrently Assertion | | | X |
| Run Assertions for Each Item Assertion | | | X |
| Set Context Variable Assertion | | | X |
| Split Variable Assertion | | | X |
| Stop Processing Assertion | | | X |
| **Threat Protection Assertions** | | | X |
| **Internal Assertions** | | X | |

| Assertion | Enforcing | Unevaluated Functional | Unevaluated Security |
|---|---|---|---|
| **Custom Assertions** | | | X |

# 3 Security Problem Definition

## 3.1 Threats

48 Table 4 identifies the threats drawn from the ESM Policy Manager PP.

**Table 4: Threats (ESM Policy Manager PP)**

| Identifier | Description |
|---|---|
| T.ADMIN_ERROR | An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms. |
| T.CONDTRADICT | A careless administrator may create a policy that contains contradictory rules for access control enforcement. |
| T.EAVES | A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data. |
| T.FORGE | A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product. |
| T.MASK | A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded. |
| T.UNAUTH | A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions. |
| T.WEAKIA | A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials. |
| T.WEAKPOL | A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity. |

49 Table 5 identifies the threats drawn from the ESM Access Control PP.

**Table 5: Threats (ESM Access Control PP)**

| Identifier | Description |
|---|---|
| T.DISABLE | A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data. |
| T.EAVES | A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data. |
| T.FALSIFY | A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy. |
| T.FORGE | A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior. |
| T.MASK | A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded. |
| T.NOROUTE | A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors. |
| T.OFLOWS | A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior. |
| T.UNAUTH | A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system. |

## 3.2 Organizational Security Policies

50 Table 6 identifies the Organizational Security Policies (OSPs) drawn from the ESM Policy Manager PP.

**Table 6: OSPs (ESM Policy Manager PP)**

| Identifier | Description |
|---|---|
| P.BANNER | The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. |

51 Table 7 identifies the OSPs drawn from the ESM Access Control PP.

**Table 7: OSPs (ESM Access Control PP)**

| Identifier | Description |
|---|---|

| Identifier | Description |
|---|---|
| P.UPDATEPOL | The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data. |

## 3.3 Assumptions

52 Table 8 identifies the assumptions drawn from the ESM Policy Manager PP.

**Table 8: Assumptions (ESM Policy Manager PP)**

| Identifier | Description |
|---|---|
| A.CRYPTO | The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services. |
| A.ESM | The TOE will be able to establish connectivity to other ESM products in order to share security data. |
| A. ROBUST | The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication. |
| A.SYSTIME | The TOE will receive a reliable time data from the Operational Environment. |
| A.USERID | The TOE will receive identity data from the Operational Environment. |
| A.MANAGE | There will be one or more competent individuals assigned to install, configure, and operate the TOE. |

53 Table 9 identifies the assumptions drawn from the ESM Access Control PP.

**Table 9: Assumptions (ESM Access Control PP)**

| Identifier | Description |
|---|---|
| A.CRYPTO | The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services. |
| A.ESM | The TOE will be able to establish connectivity to other ESM products in order to share security data. |
| A.POLICY* | The TOE will receive policy data from the Operational Environment. |
| A. ROBUST | The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication. |
| A.SYSTIME | The TOE will receive a reliable time data from the Operational Environment. |
| A.USERID | The TOE will receive identity data from the Operational Environment. |

| Identifier | Description |
|---|---|
| A.INSTALL | There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE. |

54 ***Note:** The assumption A.POLICY is included for PP conformance; however, it is addressed by the requirements of the ESM Policy Manager PP – see security objective O.POLICY. The Policy Manager provides policy data.

# 4 Security Objectives

## 4.1 Objectives for the Operational Environment

55 Table 10 identifies the objectives for the operational environment drawn from the ESM Policy Manager PP.

**Table 10: Operational environment objectives (ESM Policy Manager PP)**

| Identifier | Description |
|---|---|
| OE.ADMIN | There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE. |
| OE.CRYPTO | The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications. |
| OE.INSTALL | Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner. |
| OE.PERSON | Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE. |
| OE.PROTECT* | One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets. |
| OE.ROBUST | The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication. |
| OE.SYSTIME | The Operational Environment will provide reliable time data to the TOE. |
| OE.USERID | The Operational Environment shall be able to identify a user requesting access to the TOE. |

56 ***Note:** OE.PROTECT is included for PP conformance; however, it is addressed by the requirements of the ESM Access Control PP. The Gateway performs the ESM Access Control functions.

57 Table 11 identifies the objectives for the operational environment drawn from the ESM Access Control PP.

**Table 11: Operational environment objectives (ESM Access Control PP)**

| Identifier | Description |
|---|---|
| OE.CRYPTO | The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications. |
| OE.INSTALL | Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner. |

| Identifier | Description |
|---|---|
| OE.POLICY* | The Operational Environment will provide a policy that the TOE will enforce. |
| OE.PROTECT | The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data. |
| OE.SYSTIME | The Operational Environment will provide reliable time data to the TOE. |
| OE.USERID | The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF. |

58 ***Note:** The environmental objective OE.POLICY is included for PP conformance; however, it is addressed by the requirements of the ESM Policy Manager PP – see security objective O.POLICY. The Policy Manager provides policy data.

## 4.2 Objectives for the TOE

59 Table 12 identifies the security objectives for the TOE drawn from the ESM Policy Manager PP.

**Table 12: Security objectives (ESM Policy Manager PP)**

| Identifier | Description |
|---|---|
| O.ACCESSID | The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them. |
| O.AUDIT | The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users. |
| O.AUTH | The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF. |
| O.BANNER | The TOE will display an advisory warning regarding use of the TOE. |
| O.CONSISTENT | The TSF will provide a mechanism to identify and rectify contradictory policy data. |
| O.DISTRIB | The TOE will provide the ability to distribute policies to trusted IT products using secure channels. |
| O.INTEGRITY | The TOE will contain the ability to assert the integrity of policy data. |
| O.MANAGE | The TOE will provide the ability to manage the behavior of trusted IT products using secure channels. |

| Identifier | Description |
|---|---|
| O.POLICY | The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control. |
| O.PROTCOMMS | The TOE will provide protected communication channels or administrators, other parts of a distributed TOE, and authorized IT entities. |
| O.SELFID | The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment. |

60 Table 13 identifies the security objectives for the TOE drawn from the ESM Policy Manager PP.

**Table 13: Security objectives (ESM Access Control PP)**

| Identifier | Description |
|---|---|
| O.DATAPROT | The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product. |
| O.INTEGRITY | The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components. |
| O.MAINTAIN | The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy. |
| O.MNGRID | The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it. |
| O.MONITOR | The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users). |
| O.OFLOWS | The TOE will be able to recognize and discard invalid or malicious input provided by users. |
| O.PROTCOMMS | The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. |
| O.SELFID | The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival. |

# 5 Security Requirements

## 5.1 Conventions

61 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

## 5.2 Extended Components Definition

62 Table 14 identifies the extended components which are incorporated into this ST.

**Table 14: Extended Components**

| Component | Title | Source |
|---|---|---|
| ESM_ACD.1 | Access Control Policy Definition | ESM Policy Manager PP |
| ESM_ACT.1 | Access Control Policy Transmission | ESM Policy Manager PP |
| ESM_ATD.1 | Object Attribute Definition | ESM Policy Manager PP |
| ESM_ATD.2 | Subject Attribute Definition | ESM Policy Manager PP |
| ESM_EAU.2 | Reliance on Enterprise Authentication | ESM Policy Manager PP |
| ESM_EID.2 | Reliance on Enterprise Identification | ESM Policy Manager PP<br>ESM Access Control PP |
| FAU_SEL_EXT.1 | External Selective Audit | ESM Policy Manager PP |
| FAU_STG_EXT.1 | External Audit Trail Storage | ESM Policy Manager PP<br>ESM Access Control PP |
| FCS_CKM_EXT.4 | Cryptographic Key Zeroization | ESM Access Control PP |
| FCS_RBG_EXT.1 | Cryptographic Operation (Random Bit Generation) | ESM Access Control PP |
| FCS_SSH_EXT.1 | SSH | ESM Policy Manager PP<br>ESM Access Control PP |

| Component | Title | Source |
|---|---|---|
| FCS_TLS_EXT.1 | TLS | ESM Policy Manager PP<br>ESM Access Control PP |
| FMT_MOF_EXT.1 | External Management of Functions Behavior | ESM Policy Manager PP |
| FMT_MSA_EXT.5 | Consistent Security Attributes | ESM Policy Manager PP |
| FPT_APW_EXT.1 | Protection of Stored Credentials | ESM Policy Manager PP<br>ESM Access Control PP |
| FPT_FLS_EXT.1 | Failure of Communications | ESM Access Control PP |
| FPT_SKP_EXT.1 | Protection of Secret Key Parameters | ESM Policy Manager PP<br>ESM Access Control PP |
| FTA_SSL_EXT.1 | TSF-initiated session locking | ESM Policy Manager PP |

## 5.2.1 Class ESM: Enterprise Security Management

### 5.2.1.1 ESM_ACD Access Control Policy Definition

#### Family Behavior

63 The requirements of this family ensure that the TSF will have the ability to authoritatively define access control policies for use in an ESM deployment.

#### Component Leveling

64 There is only one component in this family, ESM_ACD.1. ESM_ACD.1, Access Control Policy Definition, requires the TSF to be able to define access control policies for consumption by external Access Control products.

**ESM_ACD.1** **Access Control Policy Definition**

The ESM_ACD family defines requirements for defining access control policies. This allows other ESM products to enforce their own security functions by using this attribute data. The ESM_ACD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define policies that govern the behavior of products that reside external to the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

Application Note: Example source for subject data would be a compatible Identity and Credential Management product.

Objects: [assignment: list of objects that can be used to make an access control decision and the source from which they are derived]; and

Application Note: A host-based example source for objects would be the operating system of the host on which those objects reside.

Operations: [assignment: list of operations that can be used to make an access control decision and the source from which they are derived]; and

Application Note: A host-based example source for operations would be the operating system of the host on which those objects reside. The operations performed against these objects would be the security-relevant functions of this operating system.

Attributes: [assignment: list of attributes that can be used to make an access control decision and the source from which they are derived].

Application Note: Example source for attribute data would be a compatible Identity and Credential Management product or the TOE itself.

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

### Management: ESM_ACD.1

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

a) Creation and modification of policies.

### Audit: ESM_ACD.1

66 The following actions should be auditable if ESM_ACD.1 Access control policy definition is included in the PP/ST:

a) Minimal: Creation and modification of policies.

#### 5.2.1.2 ESM_ACT Access Control Policy Transmission

### Family Behavior

67 The requirements of this family ensure that the TSF will have the ability to transfer defined access control policies to other ESM products.

### Component Leveling

68 There is only one component in this family, ESM_ACT.1. ESM_ACT.1, Access Control Policy Transmission, requires the TOE to transmit access control policy data

defined by ESM_ACD.1 to compatible and authorized ESM products external to the TSF under conditions defined by the ST author.

### ESM_ACT.1 Access Control Policy Transmission

The ESM_ACT family defines requirements for transmitting enterprise policy attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. The ESM_ACT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to distribute access control policy data to external entities.

Hierarchical to: No other components.

Dependencies: ESM_ACD.1 Access Control Policy Definition

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: [selection**:** choose one or more of: immediately following creation of a new or updated policy, at a periodic interval, at the request of a compatible Secure Configuration Management product, [assignment: other circumstances]].

Application Note: The intent of this requirement is to ensure that the TSF is transmitting access control policy information to an Access Control product in a timely manner so that there is assurance that it is enforcing an appropriate policy. If the assignment is selected, it must reflect that intent. If “at the request of a compatible Secure Configuration Management product” is selected, the ST author must indicate the compatible product(s) which are expected to be present in the evaluated configuration.

#### Management: ESM_ACT.1

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

a) Specification of the access control policy data to be transmitted.

b) Specification of the circumstances under which this data is transmitted.

c) Specification of the destinations to which this data is transmitted.

#### Audit: ESM_ACT.1

70 The following actions should be auditable if ESM ACT.1 Access control policy transmission is included in the PP/ST:

a) Minimal: Transmission of access control policy data to external processes or repositories.

### 5.2.1.3 ESM_ATD Attribute Definition

#### Family Behavior

71 The requirements of this family ensure that the TSF will have the ability to authoritatively define attributes for Operational Environment attributes that can subsequently be used for access control policy definition and enforcement.

### Component Leveling

72 There are two components in this family, ESM_ATD.1 and ESM_ATD.2. These components are not hierarchical to each other.

73 ESM_ATD.1, Object Attribute Definition, requires the TSF to be able to define some set of policy-related object attributes.

74 ESM_ATD.2, Subject Attribute Definition, requires the TSF to be able to define some set of policy-related subject attributes4. In both cases, these attributes are expected to be subsequently associated with controlled entities in the Operational Environment for use in handling access control. Examples of object attributes include security labels for use in mandatory access control (MAC) environments and protection levels that can be associated with web pages that reside within an organization's intranet. Examples of subject attributes include clearances or MAC ranges that would be associated with defined identities.

## ESM_ATD.1 Object Attribute Definition

The ESM_ATD.1 component defines requirements for specification of object attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. The ESM_ATD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with objects that reside in the Operational Environment.

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: [assignment: list of object security attributes].

Application Note: Object security attributes refer to attributes that may ultimately factor into an access control decision but are not associated with either a user or an access control policy. A TOE that defines access control policies for multi-level security may need to define security labels that can be associated with resources in order for the policy to be applicable to those resources.

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

### Management: ESM_ATD.1

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

a) Definition of object attributes.

b) Association of attributes with objects.

### Audit: ESM_ATD.1

76 The following actions should be auditable if ESM_ATD.1 Object attribute definition is included in the PP/ST:

a) Minimal: Definition of object attributes.

b) Minimal: Association of attributes with objects.

## ESM_ATD.2 Subject Attribute Definition

The ESM_ATD.2 component defines requirements for specification of subject attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. In particular, subject attributes might be maintained by an Identity Management component and consumed by the Access Control component. The ESM_ATD.2 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with subjects that reside in the Operational Environment.

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [assignment: list of subject security attributes].

Application Note: Subject security attributes refer to attributes that may ultimately factor into an access control decision and are associated with active entities under the access control policy. A TOE that defines access control policies for multi- level security may need to define security labels that can be associated with users in order for the policy to be applicable to those users.

ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

### Management: ESM_ATD.2

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

a) Definition of subject attributes.

b) Association of attributes with subjects.

### Audit: ESM_ATD.2

78 The following actions should be auditable if ESM_ATD.2 Subject attribute definition is included in the PP/ST:

a) Minimal: Definition of subject attributes.

b) Minimal: Association of attributes with subjects.

#### 5.2.1.4 ESM_EAU Enterprise Authentication

### Family Behavior

79 The requirements of this family ensure that the TSF will have the ability to interact with external entities for the purpose of authenticating administrators, users, or other subjects.

### Component Leveling

80 There are four non-hierarchical components in this family, ESM_EAU.1, ESM_EAU.2, ESM_EAU.5, and ESM_EAU.6.

81 ESM_EAU.1, Enterprise Authentication, requires the TSF to be able to receive authentication requests from a defined set of external entities, validate them by using some protocol, and returning the result of the decision to the requesting entity. ESM_EAU.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

82 ESM_EAU.2, Reliance on Enterprise Authentication, is the opposite of ESM_EAU.1. This allows the TSF to take an authentication performed in the Operational Environment and use it as if the TSF had performed the authentication itself.

83 ESM_EAU.5, Multiple Enterprise Authentication Mechanisms, allows the TSF to provide multi-factor authentication. ESM_EAU.5 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

84 ESM_EAU.6, Enterprise Re-authentication, allows the TSF to issue re-authentication challenges for established sessions. ESM_EAU.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

85 Note that ESM_EAU.5 and ESM_EAU.6 were derived from FIA_UAU.5 and FIA_UAU.6, respectively. They were each assigned the same component level as their CC part 2 counterparts to emphasize the similarities.

### ESM_EAU.2 Reliance on Enterprise Authentication

The ESM_EAU family defines requirements for facilitating enterprise user authentication. This allows other ESM products to enforce their own security functions by using this attribute data. This differs from FIA_UAU.1 and FIA_UAU.2 specified in CC Part 2 because these requirements specifically apply to a user authenticating to the TSF in order to perform activities that are mediated by the TSF. ESM_EAU.2 applies to the ability of the TSF to issue an authentication request that may be directed to the Operational Environment on behalf of a TOE user rather than being forced to perform its own authentication.

Hierarchical to: No other components.

Dependencies: ESM_EID.2 Reliance on Enterprise Identification

ESM_EAU.2.1 The TSF shall rely on [selection**:** [assignment: identified TOE component(s) responsible for subject authentication], [assignment:

identified Operational Environment component(s) responsible for subject authentication]] for subject authentication.

Application Note: If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

Application Note: If the TSF uses two different methods for authenticating two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.

### Management: ESM_EAU.2

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

a) Specification of entities used to perform authentication on behalf of the TSF.

### Audit: ESM_EAU.2

87 The following actions should be auditable if ESM_EAU.2 Reliance on enterprise authentication is included in the PP/ST:

a) Minimal: All use of the authentication mechanism.

#### 5.2.1.5 ESM_EID Enterprise Identification

### Family Behavior

88 The requirements of this family ensure that the TSF will have the ability to interact with external entities for the purpose of identifying administrators, users, or other subjects.

### Component Leveling

89 There are two non-hierarchical components in this family, ESM_EID.1 and ESM_EID.2.

90 ESM_EID.1, Enterprise Identification, requires the TSF to be able to receive identification requests from a defined set of external entities. These identification requests are then used as inputs for enterprise authentication. ESM_EID.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

91 ESM_EID.2, Reliance on Enterprise Identification, is the opposite of ESM_EID.1. This allows the TSF to accept the validity of an identity that was asserted in the Operational Environment.

**ESM_EID.2 Reliance on Enterprise Identification**

The ESM_EID family defines requirements for facilitating enterprise user identification. This allows for the subsequent execution of enterprise user authentication. This differs from FIA_UID.1 and FIA_UID.2 specified in CC Part 2 because these requirements specifically apply to a user presenting identification to the TSF in order to perform activities that are mediated by the TSF. ESM_EID.2 applies to the ability of the TSF to be presented identification from the Operational Environment and to treat this as valid rather than performing its own identification request.

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_EID.2.1 The TSF shall rely on [selection: [assignment: identified TOE component(s) responsible for subject identification], [assignment: identified Operational Environment component(s) responsible for subject identification]] for subject identification.

Application Note: If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

Application Note: If the TSF uses two different methods for identifying two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.

**Management: ESM_EID.2**

92 There are no management activities foreseen.

**Audit: ESM_EID.2**

93 There are no auditable events foreseen.

## 5.2.2 Class FAU: Security Audit

### 5.2.2.1 FAU_SEL_EXT External Selective Audit

**FAU_SEL_EXT.1 External Selective Audit**

The FAU_SEL_EXT.1 family defines requirements for defining the auditable events on an external IT entity. Auditable events refer to the situations that trigger audit data to be written as audit data defined in FAU_GEN.1. The FAU_SEL_EXT.1 requirement has been added because CC Part 2 lacks a selectable audit requirement that

demonstrates the ability of the TSF to define the auditable events for a specific external entity.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation
FMT_MTD.1 Management of TSF Data

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by [assignment: one or more entities in the Operational Environment] from the set of all auditable events based on the following attributes:

a) [selection: object identity, user identity, subject identity, host identity, event type]; and

b) [assignment: list of additional attributes that audit selectivity is based upon].

### Management: FAU_SEL_EXT.1

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

a) Specification of the external IT entity that will be configured by the TSF.

b) Specification of the auditable events for an external IT entity.

### Audit: FAU_SEL_EXT.1

95 The following actions should be auditable if FAU_SEL_EXT.1 External selective audit is included in the PP/ST:

a) Minimal: Changes to the set of events that are defined as auditable by the external entity.

#### 5.2.2.2 FAU_STG_EXT External Audit Trail Storage

### FAU_STG_EXT.1 External Audit Trail Storage

The FAU_STG_EXT family defines requirements for recording audit data to an external IT entity. Audit data refers to the information created as a result of satisfying FAU_GEN.1. This pertains to security audit because it discusses how audit data should be handled. The FAU_STG_EXT.1 requirement has been added because CC Part 2 lacks an audit storage requirement that demonstrates the ability of the TSF to write audit data to one or more specific external repository in a specific secure manner, as well as supporting the potential for local temporary storage.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation
FTP_ITC.1 Inter-TSF Trusted Channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [assignment: non-empty list of external IT entities and/or “TOE-internal storage”].

Application Note: The term “transmit” is intended to both TOE-initiation of the transfer of information, as well as the TOE transferring information in response to a request from an external IT entity.

Examples of external IT entities could be an Audit Server ESM component on an external machine, an evaluated operating system sharing the platform with the TOE, or a centralized logging component. Transmission to multiple sources is permitted.

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

**Management: FAU_STG_EXT.1**

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

a) Specification of the external IT entities that will receive generated audit data.

**Audit: FAU_STG_EXT.1**

97 The following actions should be auditable if FAU_STG_EXT.1 External audit trail storage is included in the PP/ST:

a) Basic: Establishment and disestablishment of communications with the external IT entities that are used to receive generated audit data.

## 5.2.3 Class FCS: Cryptographic Support

### 5.2.3.1 FCS_CKM_EXT.4 Cryptographic Key Zeroization

98 The FCS_CKM_EXT family defines requirements for deletion of cryptographic keys. The FCS_CKM_EXT.4 requirement has been added to provide a higher degree of specificity for key generation than the corresponding requirements in CC Part 2.

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

**Management: FCS_CKM_EXT.4**

99 There are no management actions foreseen.

**Audit: FCS_CKM_EXT.4**

100 The following actions should be auditable if FCS_CKM_EXT.4 Cryptographic Key Zeroization is included in the PP/ST:

a) Basic: Failure of the key zeroization process.

#### 5.2.3.2 FCS_RBG_EXT Random Bit Generation

### Family Behavior

101 The requirements of this family ensure that the TSF will generate random numbers in accordance with an approved cryptographic standard.

### Component Leveling

102 There is only one component in this family, FCS_RBG_EXT.1. FCS_RBG_EXT.1, Cryptographic Operation (Random Bit Generation), requires the TOE to perform random bit generation in accordance with a defined standard.

### FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)] seeded by an entropy source that accumulates entropy from [selection: choose one of: (1) one or more independent hardware-based noise sources, (2) one or more independent software-based noise sources, (3) a combination of hardware-based and software-based noise sources.].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

### Management: FCS_RBG_EXT.1

103 There are no management actions foreseen.

### Audit: FCS_RBG_EXT.1

104 The following actions should be auditable if FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) is included in the PP/ST:

a) Basic: Failure of the randomization process.

#### 5.2.3.3 FCS_SSH_EXT SSH

### Family Behavior

105 The requirements of this family ensure that the TSF will implement the SSH protocol in accordance with an approved cryptographic standard.

### Component Leveling

106 There is only one component in this family, FCS_SSH_EXT.1. FCS_SSH_EXT.1, SSH, requires the TOE to implement SSH in accordance with a defined standard.

### FCS_SSH_EXT.1 SSH

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

Application Note: The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done by adding additional detail in the TSS. In a future version of this PP, a requirement will be added regarding rekeying. The requirement will read “The TSF shall ensure that the SSH connection be rekeyed after no more than 228 packets have been transmitted using that key.”

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.

Application Note: RFC 4253 provides for the acceptance of “large packets” with the caveat that the packets should be of “reasonable length” or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining “reasonable length” for the TOE.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].

Application Note: In the assignment, the ST author can select the AES-GCM algorithms, or "no other algorithms" if AES-GCM is not supported. If AES-GCM is selected, there should be corresponding FCS_COP entries in the ST. Since the Dec. 2010 publication of NDPP v1.0, there has been considerable progress with respect to the prevalence of AES-GCM support in commercial network devices. It is likely that an updated version of this PP will be published in the future which will require AES-GCM and AES-CBC will become optional.

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN- RSA, PGP-SIGN-DSS, no other public key algorithms] as its public key algorithm(s).

Application Note: RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA “required” and allows two others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1, hmac- sha1-96, hmac-md5, hmac-md5-96].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

### Management: FCS_SSH_EXT.1

107 There are no management actions foreseen.

### Audit: FCS_SSH_EXT.1

108 The following actions should be auditable if FCS_SSH_EXT.1 SSH is included in the PP/ST:

109 a) Basic: Failure to establish a session.

110 b) Basic: Establishment/termination of a session.

#### 5.2.3.4 FCS_TLS_EXT TLS

### Family Behavior

111 The requirements of this family ensure that the TSF will implement the TLS protocol in accordance with an approved cryptographic standard.

### Component Leveling

112 There is only one component in this family, FCS_TLS_EXT.1. FCS_TLS_EXT.1, TLS, requires the TOE to implement TLS in accordance with a defined standard.

#### 5.3.6.1 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection: None

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

Application Note: The ST author must make the appropriate selections and assignments to reflect the TLS implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.

The ciphersuites to be used in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then “None” should be selected. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE. The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. Since the Dec. 2010 publication of this requirement in NDPP v1.0, there has been limited progress with respect to extending the prevalence of TLS 1.2 support in commercial products. Future publications of this PP will require support for TLS 1.2 (RFC 5246); however, it is likely the next version of this PP will not include a requirement for TLS 1.2 support, but will require that the TOE offer a means to deny all connection attempts using SSL 2.0 or SSL 3.0.

#### Management: FCS_TLS_EXT.1

113 There are no management actions foreseen.

#### Audit: FCS_TLS_EXT.1

114 The following actions should be auditable if FCS_TLS_EXT.1 TLS is included in the PP/ST:

a) Basic: Failure to establish a session.

b) Basic: Establishment/termination of a session.

## 5.2.4 Class FMT: Security Management

### 5.2.4.1 FMT_MOF_EXT External Management of Functions Behavior

### FMT_MOF_EXT.1 External Management of Functions Behavior

The FMT_MOF family defines the ability of the TSF to manage the behavior of its own functions. FMT_MOF_EXT extends this capability by defining requirements for managing the behavior of the functions of an external IT entity. In this case, the external IT entity to be managed is an ESM Access Control product. The FMT_MOF_EXT.1 requirement has been added because CC Part 2 lacks a requirement that demonstrates the ability of the TSF to manage functions of entities that are external to the TSF.

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security Roles

Application Note: The first assignment is expected to be completed with Access Control product functions that the TSF is capable of managing in addition to what is defined, if any. The second assignment is expected to be completed with one or more roles which are defined in FMT_SMR.1.

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: audited events, repository for audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage, [assignment: other functions] to [assignment: the authorized identified roles].

### Management: FMT_MOF_EXT.1

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

a) Specification of the external IT entity that will be configured by the TSF.

b) Configuration of the functions of the specified external entities.

### Audit: FMT_MOF_EXT.1

116 There are no auditable events foreseen. The activities defined by this requirement are a subset of the management functions specified in FMT_SMF.1. Because of this, auditing of all management functions that are specified in FMT_SMF.1 is sufficient to address the auditing of FMT_MOF_EXT.1.

#### 5.2.4.2 FMT_MSA_EXT Consistent Security Attributes

## FMT_MSA_EXT.5 Consistent Security Attributes

The FMT_MSA family defines the ability of the TSF to manage security attributes. FMT_MSA_EXT extends this capability by defining additional requirements for how these attributes can be managed.
FMT_MSA_EXT.5 requires the TSF to enforce the notion of consistent attributes. The ST author must define what constitutes inconsistent attributes and what behavior the TSF exhibits when such inconsistencies are detected. If the TSF is implemented in a manner that prevents inconsistences rather than merely detecting them, this can also be indicated. The FMT_MSA_EXT.5 requirement has been added because

| | |
|---|---|
| | CC Part 2 lacks a requirement for defining inconsistent attributes and how the TSF acts to prevent or detect their use. |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_MOF_EXT.1 External Management of Functions Behavior |
| FMT_MSA_EXT.5.1 | The TSF shall [selection: identify the following internal inconsistencies within a policy prior to distribution: [assignment: non-empty list of inconsistencies], only permit definition of unambiguous policies]. |
| Application Note: | The most common expected type of inconsistency is the case where one part of a policy allows a subject access to an object and another part denies the same subject access to the same object.<br><br>If the TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur, the ST author indicates that no ambiguous policies can be defined. If this is the case, it is expected that the TSS or operational guidance provides an overview of how contradictory policy is prevented by the TOE. |
| FMT_MSA_EXT.5.2 | The TSF shall take the following action when an inconsistency is detected: [selection: issue a prompt for an administrator to manually resolve the inconsistency, [assignment: other action that ensures that an inconsistent policy is not implemented]]. |
| Application Note: | If the TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur, FMT_MSA_EXT.5.2 is vacuously satisfied as it is impossible to have inconsistencies to detect. |

#### Management: FMT_MSA_EXT.5

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

a) Specification of inconsistent data to be detected or prevented by the TSF.

b) Specification of actions to be taken by the TSF when inconsistent data is detected.

#### Audit: FMT_MSA_EXT.5

118 There are no auditable events foreseen. The activities defined by this requirement are a subset of the management functions specified in FMT_SMF.1. Because of this, auditing of all management functions that are specified in FMT_SMF.1 is sufficient to address the auditing of FMT_MSA_EXT.5.

## 5.2.5 Class FPT: Protection of the TSF

### 5.2.5.1 FPT_APW_EXT Protection of Stored Credentials

#### Family Behavior

119 The requirements of this family ensure that the TSF will protect credential data from disclosure.

### Component Leveling

120 There is only one component in this family, FPT_APW_EXT.1. FPT_APW_EXT.1, Protection of Stored Credentials, requires the TOE to store credentials in non-plaintext form and to prevent the reading of plaintext credentials.

### FPT_APW_EXT.1 Protection of Stored Credentials

This SFR describes the behavior of the TOE when it must store credentials – either credentials for administrative users or credentials for enterprise users. An explicit requirement was required as there is no equivalent requirement in the Common Criteria. It was based on the requirement defined in the Network Device Protection Profile.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

### Management: FPT_APW_EXT.1

121 There are no management actions foreseen.

### Audit: FPT_APW_EXT.1

122 There are no auditable actions foreseen.

#### 5.2.5.2 FPT_SKP_EXT Protection of Secret Key Parameters

### Family Behavior

123 The requirements of this family ensure that the TSF will protect credential data from disclosure.

### Component Leveling

124 There is only one component in this family, FPT_SKP_EXT.1. FPT_SKP_EXT.1, Protection of Secret Key Parameters, requires the TOE to ensure that there is no mechanism for reading secret cryptographic data.

### FPT_SKP_EXT.1 Protection of Secret Key Parameters

This SFR describes the behavior of the TOE when handling pre-shared, symmetric, and private keys, collectively referred to here as secret key parameters. An explicit requirement was required as there is no

equivalent requirement in the Common Criteria. It was based on the requirement defined in the Network Device Protection Profile.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

### Management: FPT_SKP_EXT.1

125 There are no management actions foreseen.

### Audit: FPT_SKP_EXT.1

126 There are no auditable actions foreseen.

#### 5.2.5.3 FPT_FLS_EXT Failure of Communication

### FPT_FLS_EXT.1 Failure of Communication

This SFR describes the behavior of the TOE in the event there is a failure of the Policy Management product and TOE to communicate with one another.

Hierarchical to: No other components

Dependencies: No dependencies

FPT_FLS_EXT.1.1 The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: [selection: deny all requests, enforce the last policy received, [assignment: failure policy]].

Application Note: The extended requirement above is used by the ST author to describe the behavior of the TOE in the event there is a failure of the Policy Management product and TOE to communicate with one another. This requirement was refined to show that the notion of a —secure statell is defined for the TOE to be continued enforcement of some sort of policy. The specific nature of the policy to be enforced in this situation is to be completed by the ST author.

### Management: FPT_FLS_EXT.1

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

a) Definition of the behavior to take when a communications failure occurs.

### Audit: FPT_FLS_EXT.1

128 The following actions should be auditable if FPT_FLS_EXT.1 Failure of Communications is included in the PP/ST:

a) Basic: Failure of communication between the TOE and Policy Management product.

## 5.2.6 Class FTA: TOE Access

### 5.2.6.1 FTA_SSL_EXT TSF-initiated Session Locking

### FTA_SSL_EXT.1 TSF-initiated Session Locking

This SFR describes the behavior of the TOE when it must initiate session locks. An explicit requirement was required in order to narrow scope and to specify the locking actions that were fixed in the base requirement in the Common Criteria.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- lock the session – clear or overwrite display devices, making the current contents unreadable, disable any activity of the user's data access/display devices other than unlocking the session, and require that the user re- authenticate to the TSF prior to unlocking the session;
- terminate the session

] after an Authorized Administrator specified time period of inactivity.

#### Management: FTA_SSL_EXT.1

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

a) specification of the time of user inactivity after which lock-out occurs for an individual user;

b) specification of the default time of user inactivity after which lock-out occurs;

c) management of the events that should occur prior to unlocking the session.

#### Audit: FTA_SSL_EXT.1

130 The following actions should be auditable if FTA_SSL_EXT.1 is included in the PP/ST:

a) Minimal: Locking of an interactive session by the session locking mechanism.

b) Minimal: Successful unlocking of an interactive session.

c) Basic: Any attempts at unlocking an interactive session.

## 5.3 Functional Requirements

**Table 15: Summary of SFRs**

| Requirement | Title | Source |
|---|---|---|
| ESM_ACD.1 | Access Control Policy Definition | ESM Policy Manager PP |
| ESM_ACT.1 | Access Control Policy Transmission | ESM Policy Manager PP |
| ESM_ATD.1 | Object attribute definition | ESM Policy Manager PP |
| ESM_ATD.2 | Subject attribute definition | ESM Policy Manager PP |
| ESM_EAU.2 | Reliance on Enterprise Authentication | ESM Policy Manager PP |
| ESM_EID.2(1) | Reliance on Enterprise Identification (TOE user) | ESM Policy Manager PP |
| ESM_EID.2(2) | Reliance on Enterprise Identification (Service client) | ESM Access Control PP |
| FAU_GEN.1 | Audit Data Generation | ESM Policy Manager PP<br>ESM Access Control PP |
| FAU_SEL.1 | Selective Audit | ESM Access Control PP |
| FAU_STG.1 | Protected Audit Trail Storage (Local Storage) | ESM Access Control PP |
| FAU_SEL_EXT.1 | External Selective Audit | ESM Policy Manager PP |
| FAU_STG_EXT.1 | External Audit Trail Storage | ESM Policy Manager PP<br>ESM Access Control PP |
| FCO_NRR.2 | Enforced Proof of Receipt | ESM Access Control PP |
| FCS_CKM_EXT.4 | Cryptographic Key Zeroization | ESM Access Control PP |
| FCS_COP.1(1) | Cryptographic Operation (for Data Encryption/Decryption) | ESM Access Control PP |
| FCS_COP.1(2) | Cryptographic Operation (for Cryptographic Signature) | ESM Access Control PP |
| FCS_COP.1(3) | Cryptographic Operation (for Cryptographic Hashing) | ESM Access Control PP |
| FCS_COP.1(4) | Cryptographic Operation (for Keyed-Hash Message Authentication) | ESM Access Control PP |
| FCS_RBG_EXT.1 | Cryptographic Operation (Random Bit Generation) | ESM Access Control PP |

| Requirement | Title | Source |
|---|---|---|
| FCS_SSH_EXT.1 | SSH | ESM Policy Manager PP<br>ESM Access Control PP |
| FCS_TLS_EXT.1 | TLS | ESM Policy Manager PP<br>ESM Access Control PP |
| FDP_ACC.1 | Access Control Policy | ESM Access Control PP |
| FDP_ACF.1 | Access Control Functions | ESM Access Control PP |
| FIA_USB.1 | User-Subject Binding | ESM Policy Manager PP |
| FMT_MOF.1 | Management of Functions Behavior | ESM Policy Manager PP |
| FMT_MOF.1(1) | Management of Functions Behavior | ESM Access Control PP |
| FMT_MOF.1(2) | Management of Functions Behavior | ESM Access Control PP |
| FMT_MOF_EXT.1 | External Management of Functions Behavior | ESM Policy Manager PP |
| FMT_MSA.1 | Management of Security Attributes | ESM Access Control PP |
| FMT_MSA.3 | Static Attribute Initialization | ESM Access Control PP |
| FMT_MSA_EXT.5 | Consistent Security Attributes | ESM Policy Manager PP |
| FMT_SMF.1 | Specification of Management Functions | ESM Policy Manager PP<br>ESM Access Control PP |
| FMT_SMR.1 | Security Management Roles | ESM Policy Manager PP<br>ESM Access Control PP |
| FPT_APW_EXT.1 | Protection of Stored Credentials | ESM Policy Manager PP<br>ESM Access Control PP |
| FPT_FLS_EXT.1 | Failure of Communications | ESM Access Control PP |
| FPT_RPL.1 | Replay Detection | ESM Access Control PP |
| FPT_SKP_EXT.1 | Protection of Secret Key Parameters | ESM Policy Manager PP<br>ESM Access Control PP |
| FRU_FLT.1 | Degraded Fault Tolerance | ESM Access Control PP |
| FTA_SSL_EXT.1 | TSF-initiated Session Locking and Termination | ESM Policy Manager PP |
| FTA_SSL.4 | User-initiated termination | ESM Policy Manager PP |

| Requirement | Title | Source |
|---|---|---|
| FTA_TAB.1 | TOE Access Banner | ESM Policy Manager PP |
| FTP_ITC.1 | Inter-TSF Trusted Channel | ESM Policy Manager PP<br>ESM Access Control PP |
| FTP_TRP.1 | Trusted Path | ESM Policy Manager PP |

### 5.3.1 Enterprise Security Management (ESM)

**ESM_ACD.1 Access Control Policy Definition**

Hierarchical to: No other components.

ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

ESM_ACD.1.2 Access control policies defined by the TSF shall be capable of containing the following:

c) Subjects:
- *Service Clients (Source: Identity Provider)* and

d) Objects:
- *SOAP Web Services (Source: TOE Published Services)*; and

e) Operations:
- *Service Request (Source: Service Client)*

f) Attributes:
- *Access Control assertion attributes:*
  - *Authentication Credentials (Source: Service Client via Service Request)*
  - *User/Group (Source: Identity Provider)*
- *Service Availability assertion attributes:*
  - *Context attributes – time or day (Source: the Gateway)*
  - *Source IP address (Source: Service Client via Service Request)*

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

Dependencies: No dependencies

Application Note: The Policy Manager defines access control policies for consumption by the Gateway.

**ESM_ACT.1 Access Control Policy Transmission**

Hierarchical to: No other components.

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: immediately following creation of a new or updated policy, *no other circumstances*.

Dependencies: ESM_ACD.1 Access control policy definition

### ESM_ATD.1 Object attribute definition

Hierarchical to: No other components.

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects:

- Object: SOAP *Web Services:*
  - Attributes: *Associated policy assertions*

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

Dependencies: No dependencies.

### ESM_ATD.2 Subject attribute definition

Hierarchical to: No other components.

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects:

- Subject: *Service Clients*
  - Attributes: *Authentication Credentials, User/Group*

ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

Dependencies: No dependencies.

### ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to: No other components.

ESM_EAU.2.1 The TSF shall rely on *LDAP identity provider* for subject authentication.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

Dependencies: ESM_EID.2 Reliance on Enterprise Identification

Application Note: This SFR along with ESM_EID.2(1) applies to Policy Manager administrator identification and authentication.

### ESM_EID.2(1) Reliance on Enterprise Identification (TOE User)

Hierarchical to: No other components.

ESM_EID.2.1(1) The TSF shall rely on *LDAP identity provider* for subject identification.

ESM_EID.2.2(1) The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

Dependencies: No dependencies.

### ESM_EID.2(2) Reliance on Enterprise Identification (Service Client)

Hierarchical to: No other components.

ESM_EID.2.1(2) The TSF shall rely on *Internal Identity Provider or Federated with X.509 credentials Identity Provider* for subject identification.

ESM_EID.2.2(2) The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

Dependencies: No dependencies.

## 5.3.2 Security Audit (FAU)

### FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; *and*

b) All auditable events identified in Table 16 for the not specified level of audit; and

c) *No additional events.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *information specified in column three of Table 16*.

Dependencies: FPT_STM.1 Reliable time stamps

**Table 16: Auditable events**

| Component | Event | Additional Information |
|---|---|---|

| Component | Event | Additional Information |
|---|---|---|
| ESM_ACD.1 | Creation or modification of policy | Unique policy identifier |
| ESM_ACT.1 | Transmission of policy to Access Control products | Destination of policy |
| ESM_ATD.1 | Definition of object attributes. | Identification of the attribute defined. |
| ESM_ATD.1 | Association of attributes with objects. | Identification of the object and the attribute. |
| ESM_ATD.2 | Definition of subject attributes. | Identification of the attribute defined. |
| ESM_ATD.2 | Association of attributes with subjects. | None |
| ESM_EAU.2 | All use of the authentication mechanism | None |
| FAU_SEL.1 | All modifications to audit configuration | None |
| FAU_SEL_EXT.1 | All modifications to audit configuration | None |
| FAU_STG_EXT.1 | Establishment and disestablishment of communications with audit server | Identification of audit server |
| FCO_NRR.2 | The invocation of the non-repudiation service | Identification of the information, the destination, and a copy of the evidence provided |
| FCS_CKM.1 | None | None |
| FCS_CKM_EXT.4 | None | None |
| FCS_COP.1(1) | None | None |
| FCS_COP.1(2) | None | None |
| FCS_COP.1(3) | None | None |
| FCS_COP.1(4) | None | None |
| FCS_RBG_EXT.1 | None | None |

| Component | Event | Additional Information |
|---|---|---|
| FCS_SSH_EXT.1 | Failure to establish a session, establishment/termination of a session | Non-TOE endpoint of connection (IP address), reason for failure (if applicable) |
| FCS_TLS_EXT.1 | Failure to establish a session, establishment/termination of a session | Non-TOE endpoint of connection (IP address), reason for failure (if applicable) |
| FDP_ACC.1 | Any changes to the enforced policy or policies | Identification of Policy Management product making the change |
| FDP_ACF.1 | All requests to perform an operation on an object covered by the SFP | Subject identity, object identity, requested operation |
| FIA_SOS.1 | Rejection or acceptance by the TSF of any tested secret | None |
| FIA_SOS.1 | Identification of any changes to the defined quality metrics | The change made to the quality metric |
| FMT_MOF.1 | All modifications to TSF behavior | None |
| FMT_SMF.1 | Use of the management functions | Management function performed |
| FMT_SMR.1 | Modifications to the members of the management roles | None |
| FPT_FLS_EXT.1 | Failure of communication between the TOE and Policy Management product | Identity of the Policy Management product, Reason for the failure |
| FPT_RPL.1 | Detection of replay | Action to be taken based on the specific actions |
| FTP_ITC.1 | All use of trusted channel functions | Identity of the initiator and target of the trusted channel |
| FTP_TRP.1 | All attempted uses of the trusted path functions | Identification of user associated with all trusted path functions, if available |

### FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) event type; and

b) *no additional attributes.*

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note: The selective audit capability is exercised by the Policy Manager, not by a user directly accessing the Gateway.

### FAU_SEL_EXT.1 External selective audit

Hierarchical to: No other components.

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by *the Gateway* from the set of all auditable events based on the following attributes:

a) event type; and

b) *no additional attributes*.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note: The external selective audit capability is exercised by the Policy Manager, not by a user directly accessing the Gateway.

### FAU_STG.1 Protected Audit Trail Storage (Local Storage)

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

### FAU_STG_EXT.1 External audit trail storage

Hierarchical to: No other components.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to *a Syslog server and/or TOE-internal storage*.

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF Trusted Channel

### 5.3.3 Class FCO: Communication

#### FCO_NRR.2 Enforced proof of receipt

Hierarchical to: FCO_NRR.1 Selective proof of receipt

FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received *policies* at all times.

FCO_NRR.2.2 The TSF shall be able to relate the *software name, version, node* of the recipient of the information, and the *time sent, user, source IP, policy update message* of the information to which the evidence applies.

FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to *originator* given *30 seconds*.

Dependencies: FIA_UID.1 Timing of identification

### 5.3.4 FCS: Cryptographic Support

131 The TOE utilizes third-party cryptographic modules for all cryptographic primitives except those used for the SSH trusted path (for remote administrators) which is provided by the OS via OpenSSL. Per guidance at Annex C.8 of the ESM Policy Manager PP and Annex C.5 of the Access Control PP, cryptographic protocol SFRs are also included in accordance with FTP_ITC and FTP_TRP application notes.

#### FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys)

Hierarchical to: No other components.

FCS_CKM.1.1 Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with:

- *NIST Special Publication 800-56B, —Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography for RSA-based key establishment schemes*

and specified cryptographic key sizes ***equivalent to, or greater than, 112 bits of security*** that meet the following: ***standards defined in first selection***.

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution, or
FCS_COP.1 Cryptographic Operation]
FCS_CKM.4 Cryptographic Key Destruction

Application note: This is for RSA used by SSH.

#### FCS_CKM_EXT.4 Cryptographic Key Zeroization

Hierarchical to: No other components.

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

Dependencies: No dependencies.

Application note: This is relevant only to the destruction of keys used by SSH.

### FCS_COP.1(1) Cryptographic Operation (for Data Encryption/Decryption)

Hierarchical to: No other components.

FCS_COP.1.1(1) Refinement: The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in CBC mode* and cryptographic key sizes *128-bits, 256-bits* and *no other key size* that meets the following:

- FIPS PUB 197, —Advanced Encryption Standard (AES)
- *NIST SP 800-38A*

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or
FDP_ITC.2 Import of User Data with Security Attributes, or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction

Application note: This is for AES used by SSH.

### FCS_COP.1(2) Cryptographic Operation (for Cryptographic Signature)

Hierarchical to: No other components.

FCS_COP.1.1(2) Refinement: The TSF shall perform *cryptographic signature services* in accordance with a selection:

*(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater*

that meets the following:

*FIPS PUB 186-3, — Digital Signature Standard*.

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or
FDP_ITC.2 Import of User Data with Security Attributes, or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction

Application note: This is for RSA used by SSH.

### FCS_COP.1(3) Cryptographic Operation (for Cryptographic Hashing)

Hierarchical to: No other components.

| | |
|---|---|
| FCS_COP.1.1(3) | Refinement: The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm *SHA-1, SHA-256* and *message digest sizes 160, 256 bits* that meet the following: *FIPS Pub 180-3, —Secure Hash Standard*. |
| Dependencies: | [FDP_ITC.1 Import of User Data without Security Attributes, or<br>FDP_ITC.2 Import of User Data with Security Attributes, or<br>FCS_CKM.1 Cryptographic Key Generation]<br>FCS_CKM.4 Cryptographic Key Destruction |
| Application note: | This relates to hashing services used in SSH. |

### FCS_COP.1(4) Cryptographic Operation (for Keyed-Hash Message Authentication)

| | |
|---|---|
| Hierarchical to: | No other components. |
| FCS_COP.1.1(4) | Refinement: The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-SHA-1* key size *160 bits*, and message digest sizes *160 bits* that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, —Secure Hash Standard.* |
| Dependencies: | [FDP_ITC.1 Import of User Data without Security Attributes, or<br>FDP_ITC.2 Import of User Data with Security Attributes, or<br>FCS_CKM.1 Cryptographic Key Generation]<br>FCS_CKM.4 Cryptographic Key Destruction |
| Application note: | This relates to the HMAC used in SSH. |

### FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

| | |
|---|---|
| Hierarchical to: | No other components. |
| FCS_RBG_EXT.1.1 | The TSF shall perform all random bit generation (RBG) services in accordance with NIST Special Publication 800-90 using CTR_DRBG (AES) seeded by an entropy source that accumulates entropy from one or more independent software-based noise sources. |
| FCS_RBG_EXT.1.2 | The deterministic RBG shall be seeded with a minimum of 256 bits of entropy at least equal to the greatest security strength of the keys and hashes that it will generate. |
| Dependencies: | No dependencies. |
| Application note: | The DRBG referred to is provided by the OS OpenSSL for use in SSH. |

### FCS_SSH_EXT.1 SSH

| | |
|---|---|
| Hierarchical to: | No other components. |
| FCS_SSH_EXT.1.1 | The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254. |

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than *32768* bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, no other algorithms.

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and PGP-SIGN-RSA as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is hmac-sha1, hmac- sha1-96.

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

Dependencies: FCS_COP.1 Cryptographic Operation

**FCS_TLS_EXT.1 TLS**

Hierarchical to: No other components.

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols TLS 1.2 (RFC 5246) supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Dependencies: FCS_COP.1 Cryptographic Operation

### 5.3.5 Class FDP: User Data Protection

**FDP_ACC.1 Access Control Policy**

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *access control Security Function Policy (SFP)* on

- Subjects: *Service Clients (on behalf of users)*
- Objects: SOAP *Web Services*; and
- Operations: *Service Request*

Dependencies: FDP_ACF.1 Security attribute based access control

Application note: The Gateway enforces the access control SFP.

**FDP_ACF.1 Access Control Functions**

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the *access control SFP* to objects based on the following: *all operations between users and objects based upon the attributes defined in ESM_ACD.1*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules received from the Policy Manager.*

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *if a requested object is not explicitly allowed by policy, then the access to the requested object is denied by default*.

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

### 5.3.6 Class FIA: Identification and Authentication

**FIA_USB.1 User-subject binding**

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *username*, *role*.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- *The TSF determines the username from the credentials presented for authentication.*
- *The TSF associates the role with the corresponding username*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *Once a user's session is established, the security attributes associated with a subject acting on behalf of a user cannot be changed for the duration of that user's session.*

Dependencies: FIA_ATD.1 User attribute definition

Application note: This requirement refers to TOE administrative users.

### 5.3.7 Class FMT: Security Management

**FMT_MOF.1 Management of Functions Behavior**

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions: *functions in Table 17* to *roles in Table 18 according to the operations and attributes for each role in Table 18*.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security Roles

**FMT_MOF.1(1) Management of Functions Behavior**

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions: *audited events, repository for trusted audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage*, *no other functions* to *an authorized and compatible Policy Management product.*

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

**FMT_MOF.1(2) Management of Functions Behavior**

Hierarchical to: No other components.

FMT_MOF.1.1(2) The TSF shall restrict the ability to determine the behavior of the functions: *policy being implemented by the TSF*, *no other functions* to *an authorized and compatible Enterprise Security Management product.*

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

**FMT_MOF_EXT.1 External management of functions behavior**

Hierarchical to: No other components.

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products*:* audited events, repository for remote audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage to **the roles** *Administrator (query and modify), Operator (query only)*.

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

Application note: The TOE supports numerous roles (refer to Table 18) of which the Administrator and Operator are the superset.

### FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall shall enforce the *access control SFP* to restrict the ability to change_default, query, modify, delete the security attributes *access control policies, access control policy attributes, implementation status of access control policies* to *an authorized and compatible Policy Management product*.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

### FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the *access control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *authorized and compatible Policy Management product* to specify alternative initial values to override the default values when an object or information is created.

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

### FMT_MSA_EXT.5 Consistent security attributes

Hierarchical to: No other components.

FMT_MSA_EXT.5.1 The TSF shall identify the following internal inconsistencies within a policy prior to distribution: *incorrect assertion order, syntax errors and unfulfilled dependencies*.

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: issue a prompt for an administrator to manually resolve the inconsistency.

Dependencies: FMT_MOF_EXT.1 External Management of Functions Behavior

### FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: *configuration of audited events, configuration of repository for trusted audit storage, configuration of Access Control SFP, querying of policy being implemented by the TSF, management of Access Control*

*SFP behavior to enforce in the event of communications outage and activities listed in Table 17*.

Dependencies: No dependencies.

**Table 17: Management Functions within the TOE**

| Requirement | Management Activities |
|---|---|
| ESM_ACD.1 | Creation of policies |
| ESM_ACT.1 | Transmission of policies |
| ESM_ATD.1 | Definition of object attributes.<br>Association of attributes with objects. |
| ESM_ATD.2 | Definition of subject attributes.<br>Association of attributes with subjects. |
| ESM_EAU.2 | Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF) |
| ESM_EID.2 | Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF) |
| FAU_SEL.1 | Configuration of auditable events |
| FAU_SEL_EXT.1 | Configuration of auditable events for defined external entities |
| FAU_STG_EXT.1 | Configuration of external audit storage location |
| FIA_USB.1 | Definition of default subject security attributes, modification of subject security attributes |
| FMT_MOF_EXT.1 | Configuration of the behavior of other ESM products |
| FMT_MSA_EXT.5 | Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected |
| FMT_SMR.1 | Management of the users that belong to a particular role |
| FTA_TAB.1 | Maintenance of the banner |
| FTP_ITC.1 | Configuration of actions that require trusted channel |
| FTP_TRP.1 | Configuration of actions that require trusted path |

### FMT_SMR.1 Security Management Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles *defined in Table 18.*

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

Dependencies: FIA_UID.1 Timing of Authentication

**Table 18: Roles and permissions**

| Role | Operations | Attributes |
|---|---|---|
| Administrator | Any | Policy Manager – All |
| Operator | Read | Policy Manager – All |
| ssgconfig | Any | Gateway Configuration Utility – All |
| root | Any<br>**Note:** In the evaluated configuration, root is not used to configure / access the TOE. The ssgconfig account is used for this purpose. | Gateway Configuration Utility – All<br>Privileged Shell (CLI) – All |
| Gateway Maintenance | Create, read, and update | FTP Audit Archiver (used to back up the audit logs on the Gateway via FTP to a specified host) |
| Invoke Audit Viewer Policy | Read | Audit events |
| Manage [name] Folder | Read, update, and delete | Policies within a defined folder |
| Manage [name] Identity Provider | Read, update, and delete | Identity Provider (with a defined name) |
| Manage[name] Policy | Read, update, and delete | Named Policy |
| Manage [name] Service | Delete, view, update | Web Service<br>Assertions for web service policies |
| Manage Administrative Accounts Configuration | Create, read, and update | Cluster properties applicable to administrative account configuration: logon.maxAllowableAttempts<br>logon.lockoutTime<br>logon.sessionExpiry<br>logon.inactivityPeriod. |
| Manage Certificates | Create, read, update, and delete | Trusted certificates<br>Policies for revocation checking |

| Role | Operations | Attributes |
|---|---|---|
| Manage Cluster Properties | Create, read, update, and delete | Cluster status information |
| Manage Internal Users and Groups | Create, read, update, and delete | Users<br>Groups (used to organize users as a time-saving tool) |
| Manage Listen Ports | Create, read, update, and delete | Gateway listen ports (both HTTP(S) and FTP(S)) |
| Manage Log Sinks | Create, read, update, and delete | Log sinks (manage where audit records should be sent) |
| | Read | Folders<br>Identity Providers<br>Listen ports<br>Log files<br>Policies<br>Services<br>Users |
| Manage Password Policies | Read and update | Password policy |
| Manage Private Keys | Create, read, update, and delete | Private keys<br>Default SSL key<br>Default CA key |
| Manage Secure Passwords | Read, create, update, and delete | Stored passwords |
| Manage UDDI Registries | Create, read, update, and delete | UDDI registries<br>**Note:** UDDI not within scope of the TOE. This role is listed for completeness. |
| Manage Web Services | Publish, edit, delete | Web Service |
| | Read | Existing Users |
| | Edit | Global Policy<br>Assertions for web service policies |
| Publish External Identity Providers | Create | External Identity Provider |

| Role | Operations | Attributes |
|---|---|---|
| Publish Web Services | Publish | Web Service |
| Search Users and Groups | Read | Users and Groups |
| View [name] Folder | Read | Policies within a defined folder |
| View [name] Log Sink | Read | Audit events |
| View Audit Records | Read | Audit events |

**Note:** For additional detail related to roles and terms above, refer to *Predefined Roles and Permissions* in the *Online Documentation*.

Application Note: Annex A: Access Control Matrix provides a mapping between the roles that the TOE implements and the management functions specified by FMT_SMF.1.

### 5.3.8 Class FPT: Protection of the TSF

#### FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to: No other components.

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

Dependencies: No dependencies.

#### FPT_FLS_EXT.1 Failure of Communications

Hierarchical to: No other components.

FPT_FLS_EXT.1.1 The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: enforce the last policy received.

Dependencies: No dependencies.

#### FPT_RPL.1 Replay Detection

Hierarchical to: No other components.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *TLS protected data*.

FPT_RPL.1.2 The TSF shall perform *reject the data* when replay is detected.

Dependencies: No dependencies.

**FPT_SKP_EXT.1 Protection of Secret Key Parameters**

Hierarchical to: No other components.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Dependencies: No dependencies.

Application Note: The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through “normal” interfaces. While it is understood that the administrator could directly read memory to view these keys, do so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not endeavor in such an activity.

### 5.3.9 Class FRU: Resource Utilization

**FRU_FLT.1 Degraded fault tolerance**

Hierarchical to: No other components.

FRU_FLT.1.1 The TSF shall ensure the operation of *enforcing the most recent policy* when the following failures occur: *restoration of communications with the Policy Management product after an outage*.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

### 5.3.10 Class FTA: TOE Access

**FTA_TAB.1 TOE access banner**

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display ~~**an**~~ **a configurable** advisory warning message regarding unauthorized use of the TOE.

Dependencies: No dependencies.

Application note: This is only relevant to the Policy Manager interface.

**FTA_SSL_EXT.1 TSF-initiated session locking**

Hierarchical to: No other components

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions,

- terminate the session

after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies

Application note: This requirement is only applicable to the Policy Manager.

### FTA_SSL.4 User-initiated termination

Hierarchical to: No other components

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

Dependencies: No dependencies

## 5.3.11 Class FTP: Trusted Paths/Channels

### FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall **use TLS to** provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and 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 *transfer of policy data, service client connections, Syslog server communication, LDAP server communication.*

Dependencies: No dependencies.

Application note: Use of TLS for service client connections is optional based on the configuration specified by the administrator. This is achieved via use of the 'Require SSL or TLS Transport Assertion'.

### FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall **use SSH to** provide a **trusted** communication path between itself and remote users that is logically distinct from other communication ~~**paths**~~ **channels** and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, *execution of management functions*.

Dependencies: No dependencies.

## 5.4 Assurance Requirements

132 The TOE security assurance requirements, summarized in Table 19, are drawn from the claimed Protection Profiles.

**Table 19: Assurance Requirements**

| Assurance Class | Components | Description |
|---|---|---|
| Development | ADV_FSP.1 | Basic Functional Specification |
| Guidance Documents | AGD_OPE.1 | Operational User Guidance |
| | AGD_PRE.1 | Preparative User Guidance |
| Tests | ATE_IND.1 | Independent Testing – conformance |
| Vulnerability Assessment | AVA_VAN.1 | Vulnerability Analysis |
| Life Cycle Support | ALC_CMC.1 | Labelling of the TOE |
| | ALC_CMS.1 | TOE CM Coverage |

# 6 TOE Summary Specification

## 6.1 Access Control Policy Definition

| **Related SFRs:** | ESM_ACD.1, ESM_ATD.1, ESM_ATD.2, FMT_MOF.1, FMT_MSA_EXT.5, FMT_SMF.1, FMT_MOF_EXT.1 |
|---|---|

133 This security function refers to the access control policy definition capabilities of the Policy Manager. The Policy Manager is used to configure and define access control policies for the CA API Gateway (i.e. the Gateway is the compatible access control product). A summary of the policy definition capability is provided below however the *Policy Assertions* section of *the Online Documentation* is dedicated to this topic and should be referenced for detailed information.

134 A policy defines restrictions for the consumption of a published Gateway-protected service. At the highest layer of abstraction, the attributes used in policy definition are as defined in ESM_ACD.1. Details for included policy assertions are provided in sections 6.1.1, 6.1.2 and 6.1.3 below.

135 In the Policy Manager, a service policy includes assertions that determine the authentication method, identity credentials, transport method, and routing method for the web service. The specific types of assertions, their relative location, and the other assertions determine the properties and validity of a policy. During processing, the Gateway scans each policy assertion from top to bottom, assigning a 'succeed' or 'fail' outcome to each.

136 Policies are constructed in a 'policy development window' by moving assertions and policy fragments (template groups of assertions) into a meaningful tree structure resulting in '1$^{st}$ level' and 'child' assertions. There are two special assertions used to refine policy logic:

a) **At least one assertion must evaluate to true folder.** Each child assertion placed in this folder is processed until an assertion succeeds. At this point, processing of the folder stops and the "At least one" folder is assigned a successful outcome. However if all assertions in the folder fail, then the "At least one" assertion is assigned a failure outcome.

b) **All assertions must evaluate to true folder.** Each child assertion placed in this folder is processed until an assertion fails. At this point, processing of the folder stops and the "All assertions" folder is assigned a failure outcome. However if all assertions in the folder succeed, then the "All assertions" folder is assigned a successful outcome.

137 The TOE restricts the ability to manage security attributes in accordance with Table 18 and provides the management capabilities defined in the *Online Documentation*.

138 Policy values are restrictive by default – access to objects is denied unless the administrator defines a policy to enable access.

139 Policy consistency checking is performed by the Policy Validator within the Policy Manager. The Policy Validator detects syntax errors, unfulfilled dependencies and incorrect ordering of assertions. The administrator is notified when an error is detected. The Policy Validator is not configurable.

140 The Policy Manager can keep a revision history of changes made to a policy or policy fragment. It can record when a change was made and who made it. A version number is assigned to each change. You can roll back to any version, making it the "active" policy. This functionality is described in the *Policy Revisions* section of the *Online Documentation.*

### 6.1.1 Access Control Assertions

141 The following subset of assertions are evaluated:

a) **Authenticate User or Group.** Require specified users and/or groups to be authenticated against a selected identity provider. Applies the credentials collected by a 'require' assertion listed below to authenticate a user or group specified in this 'authenticate' assertion. Refer to *Authenticate User or Group Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

b) **Authenticate against Identity Provider.** Requires provided client credentials to be successfully authenticated against a selected identity provider. Applies the credentials collected by the 'require' assertions to be authenticated. Refer to *Authenticate against Identity Provider Assertion* section of the *Online Documentation* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the following Identity Providers are supported:

   i) Internal

   ii) Federated with X.509 credentials

c) **Require HTTP Basic** (**Note:** should be used in conjunction with Require SSL or TLS). Require that incoming requests to contain HTTP basic authentication credentials. Refer to *Require HTTP Basic Credentials Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

d) **Require SAML Token Profile.** Requires incoming requests to contain a SAML token. Refer to *Require SAML Token Profile Assertion* section of the *Online Documentation* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the allowable attributes are as follows:

   i) **SAML Version.** SAML v2

   ii) **SAML Statement Type.** Authentication

   iii) **Authentication Methods.** Password, Password Protected Transport, SSL/TLS Client Certificate authentication, X.509 Public Key, XML Digital Signature

   iv) **Authorization Statement.** Not applicable

   v) **Attribute Statement.** Not applicable

   vi) **Subject Confirmation.** Sender Vouches (SV) or Holder-of-Key (HOK)

   vii) **Name Identifier.** Any

   viii) **Conditions.** Check Assertion Validity Period.

e) **Require SSL or TLS Transport with Client Authentication.** Requires clients to connect via SSL or TLS and to provide a valid / trusted X.509 certificate. Refer to *Require SSL or TLS Transport Assertion* section of the *Online Documentation* for a list of related attributes and behavior.
**Note:** This assertion appears in two different assertion palettes:

   i) When accessed from the Access Control palette, this assertion is labeled "Require SSL or TLS Transport with Client Authentication" and has the Require Client Certificate Authentication check box selected by default.

ii) When access from the Transport Layer Security palette, this assertion is labeled “Require SSL or TLS Transport” and does not have the Require Client Certificate Authentication check box selected by default.

f) **Require WS-Security Signature Credentials.** Requires that the web service target message includes an X.509 client certificate and has at least one element signed by that client certificate’s private key as a proof of possession. Refer to *Require WS-Security Signature Credentials Assertion* section of the *Online Documentation* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the allowable attributes are as follows:

i) **Allow multiple signatures.** Disabled / unchecked

ii) **Signature element variable.** Disabled / unchecked

iii) **Signature reference element variable.** Disabled / unchecked

### 6.1.2 Service Availability Assertions

142 The following subset of service availability assertions are evaluated:

a) **Limit Availability to Time/Days.** Enables restricting service access by a time and/or day interval. When the Gateway receives a request for the service, it will check the time and/or day restrictions before allowing the message to proceed. Refer to *Limit Availability to Time/Days Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

b) **Restrict Access to IP Address Range.** Enables restricting service access based on the IP address of the requesting service client. Refer to *Restrict Access to IP Address Range Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

### 6.1.3 Policy Logic Assertions

143 The following subset of policy logic assertions are evaluated in support of the above assertions:

a) **All Assertions Must Evaluate to True.** The “All assertions must evaluate to true” assertion is a folder that organizes and defines the processing conditions for the assertions that it contains and for the overall policy. When assertions are grouped into one of these folders, each successive child assertion is processed until all assertions succeed, yielding a success outcome for the folder. Processing in this assertion folder will stop when the first child assertion fails, yielding a fail outcome for the folder. Refer to *All Assertions Must Evaluate to True Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

b) **At Least One Assertion Must Evaluate to True.** The “At least one assertion must evaluate to true” assertion is a folder that organizes and defines the processing conditions for the assertions that it contains and for the overall policy. When assertions are grouped into one of these folders in the policy window, each successive child assertion is processed until a single assertion succeeds, yielding a success outcome for the folder. If all child assertions in the folder fail, then the overall folder fails. Refer to *At Least One Assertion Must Evaluate to True Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

## 6.2 Access Control Policy Enforcement

| **Related SFRs:** | ESM_EID.2(2), FDP_ACC.1, FDP_ACF.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FCS_TLS_EXT.1, FTP_ITC.1 |
|---|---|

144 The Gateway enforces polices defined by the Policy Manager (see section 6.1 for policy types). In the evaluated configuration, the Gateway may only consume policies from the TOE Policy Manager although it is compatible with other means as described in section 2.3.3. The Gateway authenticates the Policy Manager using TLS endpoint authentication (refer to section 6.7 for TLS details).

145 The Gateway performs the following message processing for a typical policy:

a) Service request arrives.

b) Request is run through the WS-Security processor:

   i) Encrypted sections are decrypted and WS-Security Signatures are verified. The sign and/or encrypt order is chosen by the sender (in the evaluated configuration, only signature verification is applicable when SAML envelope signatures are in use).

   ii) Default security header can be optionally removed before routing

c) Request is run through the policy assertions in linear order

d) Response is run through the WS-Security decorator:

   i) Default security header is created

   ii) Signatures specified by the policy are applied (only applicable for SAML envelope signatures)

   iii) Encryption specified by the policy is performed (not applicable in the evaluated configuration).

e) Response is sent back to the client.

146 All first level assertions in a policy (including first level “At least” and “All assertions” folders) must succeed in order for the overall policy to succeed. When the policy succeeds, the service requestor receives a response message. If the policy fails, the service requestor receives an error message.

147 Initial Gateway configuration is performed using the Gateway Configuration Utility, described in the *Gateway Main Menu (Appliance)* section of the *Online Documentation.* Subsequent to initial setup, configuration in performed by the Policy Manager.

148 The Gateway Configuration Utility recognizes only the ssgconfig and root roles, however in the evaluated configuration, only the ssgconfig role is used to configure the TOE. The TOE restricts the ability to manage security attributes in accordance with Table 18.

149 Policy values are restrictive by default – access to objects is denied unless the administrator defines a policy to enable access.

150 Communication with service clients is protected using TLS. Refer to section 6.7 for TLS details.

### 6.2.1 Enterprise Identification

151 Per ESM_EID.2(1), when the *Authenticate against Identity Provider* assertion is included in the policy to be enforced, the TOE requires provided client credentials to

be successfully authenticated against a selected identity provider. Refer to *Authenticate against Identity Provider Assertion* section of the *Online Documentation* for a list of related attributes and behavior. In the evaluated configuration (specified by the *Secure Installation Guide*), the following Identity Providers are supported:

a) Internal

b) Federated with X.509 credentials

## 6.3 Policy Security

**Related SFRs:** ESM_ACT.1, FCS_TLS_EXT.1, FTP_ITC.1, FPT_RPL.1, FCO_NRR.2

152 The Policy Manager transmits policies to the Gateway immediately after creation. A trusted channel (TLS) is established between the Policy Manager and the Gateway to protect the transmission of policy data. TLS provides replay detection and will reject the replayed packets and generate an audit event when detection occurs. TLS also provides certificate based mutual authentication between the Policy Manager and the Gateway.

153 Access to the Policy Manager and the Gateway requires user identification and authentication (username & password) as described in section 6.5.

154 The Policy Manager is a thick client Java application executed on a general purpose operating system. Remote access to the Policy Manager application is not supported. The Gateway Configuration Utility may be accessed locally or remotely. Remote access is secured using SSH (refer to section 6.7 for detail).

155 The TOE relies on FIPS validated third-party cryptographic modules for TLS as identified in section 2.3.2. Refer to section 6.7 for TLS details.

156 The Gateway generates an audit record when a policy is received from the Policy Manager, providing proof of receipt. Refer to *Gateway Confirmation of Policy Versions* section of the *Security Installation Guide* for the contents and formatting of the receipt / audit record. The Policy Manager is used to view generated audit records. As documented above, the Policy Manager and Gateway are mutually authenticated using TLS certificates. The ‘node’ field of the receipt identifies the name of the Gateway to which the policy was applied.

## 6.4 System Monitoring

**Related SFRs:** FAU_GEN.1, FAU_SEL.1, FAU_SEL_EXT.1, FAU_STG.1, FAU_STG_EXT.1, FCS_TLS_EXT.1, FTP_ITC.1

157 The TOE generates the audit events identified in Table 16 (a full list of TOE audit message codes is provided in the Audit Detail Codes section of the *Online Documentation*). The TOE may store logs in an internal database or an external Syslog server. Communication with the Syslog server is secured using TLS (refer to section 6.7 for detail).

158 Authorized users may view audit events via the Policy Manager. The set of events to be audited may be filtered based on event type. Event type is based on Severity Level (INFO, WARNING, SEVERE) with allowable selections being as follows: Selectable is INFO and WARNING | Non-Selectable is SEVERE (i.e. SEVERE is always logged). Additional details are provided in the *Overriding the Audit Level* section of the *Online Documentation.*

159 Audit logs cannot be modified via the Policy Manager. The Administrator may delete audit events that are more than 7 days old. Audit events are recorded until a

predefined percentage of the database hard disk space is consumed. Once the threshold is reached, all message processing ceases until the log size drops below the threshold. The threshold is defined in the *audit.archiverShutdownThreshold* cluster property and is 90% by default.

160 Additional detail regarding the audit functionality is provided in the *Gateway Audit Events* section of the *Online Documentation*.

161 Detail regarding the local system logs on the Gateway appliance is available at the following sections of the *Online Documentation*:

a) *View Logs for the Gateway*

b) *Configuring the Gateway Logging Functionality*

162 By default, these local system logs consist of 10 log files of 20 MB each, which are used and rolled over as they fill up.

163 The TOE synchronizes time with an NTP server. For configuration details, refer to *Gateway System Settings (Appliance)* of the *Online Documentation*.

164 When configured in accordance with the *Secure Installation Guide,* the following policy assertions are used in support of system monitoring:

a) **Audit Message in Policy.** Enables auditing of messages within a policy. It records events pertaining to the processing of a policy— e.g. assertion violations. Refer to the *Audit Messages in Policy Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

b) **Add Audit Detail.** Allows the definition of a custom message that can enhance the context of an audit message. Refer to the *Add Audit Detail Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

c) **Customize SOAP Fault Response.** Allows customization of the SOAP fault response on a policy-by-policy basis. Refer to the *Customize SOAP Fault Response Assertion* section of the *Online Documentation* for a list of related attributes and behavior.

## 6.5 Secure Administration

| **Related SFRs:** | ESM_EAU.2, ESM_EID.2(1), FCS_SSH_EXT.1, FTA_SSL_EXT.1, FTA_SSL.4, FIA_USB.1, FMT_SMR.1, FTP_TRP.1, FTA_TAB.1, FPT_APW_EXT.1, FPT_SKP_EXT.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1 |
|---|---|

165 Access to the TOE can be achieved via the Policy Manager application or the Gateway Configuration Utility. Users must authenticate prior to being granted access. Users may authenticate via username and password.

166 The Policy Manager administrative user database may be:

a) **LDAP identity provider - MSAD (Microsoft Active Directory).** User details are maintained on an external MSAD identity server (refer to the *LDAP Identity Providers* section of the *Online Documentation*).

167 The Gateway is configured via the Gateway Configuration Utility which is typically only performed when the TOE is first deployed and subsequent management is performed via the Policy Manager. The Gateway makes use of local user accounts – ssgconfig and root. In accordance with the evaluated configuration specified in the *Secure Installation Guide* the root account may not be used while the TOE is in an operational state.

168 The TOE determines the username from the credentials presented at authentication and associates the defined role with the corresponding username. The TOE maintains the roles and associated access permissions defined in Table 18. For configuration details refer to the *Manage Roles* section of the *Online Documentation.*

169 The TOE terminates inactive local sessions at the Policy Manager after an administrator defined period of inactivity. The period of inactivity for session timeout may be set between 1 and 1440 minutes and the default is 30 minutes. Users may also terminate their own session. For configuration details refer to *Managing Password Policy* section of the *Online Documentation*.

170 The Policy Manager is a thick client Java application executed on a general purpose operating system. Remote access to the Policy Manager application is not supported. The Gateway Configuration Utility may be accessed locally or remotely. Remote access is secured using SSH (refer to section 6.7 for SSH details including related cryptography).

171 The TOE displays an administrator defined banner at logon to the Policy Manager. For configuration details, refer to the *Administrative Account Cluster Properties* section of the *Online Documentation*.

### 6.5.1 Protection of Stored Keys and Credentials

172 Table 20 below identifies the secret keys and credentials stored by the TOE and describes how they are protected from disclosure in accordance with FPT_APW_EXT.1 and FPT_SKP_EXT.1.

**Table 20: Keys and Credentials**

| Name | Description | Protection |
|---|---|---|
| LDAP User Passwords | Policy Manager user passwords. | Not stored or managed by the TOE. |
| Local User Passwords | Gateway ssgconfig and root account passwords<br>**Note:** In the evaluated configuration, root is not used to configure / access the TOE. The ssgconfig account is used for this purpose. | SHA-512 hash stored by the OS. |
| Service Client Stored Passwords | The TOE is able to store passwords and plaintext PEM encoded private keys on behalf of service clients.<br>Refer to *Manage Stored Passwords* in the *Online Documentation* | Stored in encrypted fields in the Internal DB using AES-256 (CBC).<br>TOE logic prevents display of plaintext passwords and PEM keys to users. |
| Service Client Stored Keys | The TOE is able to store asymmetric private keys on behalf of Service Clients.<br>Refer to *Manage Private Keys* in the *Online Documentation.* | Stored in encrypted PKCS#12 keystore in the Internal DB using AES-256 (CBC) or protected by the HSM if in use. |

| Name | Description | Protection |
|---|---|---|
| Gateway SSH Server Private Key | Plain text SSH server host key. | Stored in a protected file on the Gateway OS with root access only.<br>The administrator may zeroize this key using the shred command. This causes a three pass overwrite of the file holding the key. |
| Gateway TLS Private Key | TLS static private key used for communication with the Policy Manager. | Stored in encrypted PKCS#12 keystore in the Internal DB using AES-256 (CBC) or protected by the HSM if in use. |
| Policy Manager TLS Private Key | TLS static private key used for communication with the Gateway. | Key is stored within a directory in the OS users home directory (of the machine the Policy Manager is running on) in the trustStore file which is a Java JKS keystore that is obscured using a Sun proprietary algorithm. |
| Cluster Shared Key | Use to derive Internal DB encryption keys. | Stored in the Internal DB - encrypted with the cluster-passphrase using Password Based Encryption (PBEWithSHA1AndDESede) |
| Cluster Passphrase | Used to protect the cluster shared key per above. | Stored in Gateway properties file – encrypted with AES-CBC. |

## 6.6 Continuity of Enforcement

**Related SFRs:** FPT_FLS_EXT.1, FRU_FLT.1, FMT_MOF_EXT.1

173 The Gateway continues policy enforcement in the event of a loss of connectivity with the Policy Manager by enforcing the last policy received. Continuous connectivity with the Policy Manager is not expected or required. Creation of new policies requires connectivity to the Gateway as it stores the policy data on an internal database. This behavior is not configurable.

## 6.7 TLS and SSH Details

174 This section provides additional detail regarding the TOE's implementation of TLS and SSH.

### 6.7.1 TLS

175 The TOE makes use of TLS in the following ways:

a) Between service clients and the Gateway – in this case the TOE is a TLS server.

b) Between the Policy Manager and the Gateway – in this case the TOE is both a TLS client (Policy Manager) and TLS server (Gateway).

c) Between the Gateway and a Syslog server – in this case the TOE is a TLS client.

d) Between the Gateway and an LDAP server (Microsoft Active Directory used for Policy Manager user database) – in this case the TOE is a TLS client.

176 The TLS implementation has the following characteristics when configured in accordance with the *Secure Installation Guide*:

a) TLS 1.2 (RFC 5246) is supported without extensions.

b) Client authentication is supported (i.e. if configured the client must submit a trusted certificate to the server).

c) When acting as either client or server, the TOE is configured to negotiate the following ciphersuites in the following order of preference, if a listed ciphersuite is not supported by the other party then the connection will be refused:

i) TLS_RSA_WITH_AES_256_CBC_SHA

ii) TLS_RSA_WITH_AES_128_CBC_SHA

iii) TLS_DHE_RSA_WITH_AES_128_CBC_SHA

iv) TLS_DHE_RSA_WITH_AES_256_CBC_SHA

177 The underlying cryptography for TLS is provided by third-party cryptographic modules per section 6.8.

### 6.7.2 SSH

178 The TOE makes use of SSH to secure remote administrator access to the Gateway.

179 The SSH implementation has the following characteristics when configured in accordance with the *Secure Installation Guide*:

a) The TOE implements SSHv2

b) Password authentication is supported

c) SSH_RSA and PGP-SIGN-RSA are supported for authentication

d) Packets greater than 32768 bytes in an SSH transport connection are dropped

e) The TOE supports the following SSH encryption algorithms:

i) AES-CBC-256

ii) AES-CBC-128

f) In FIPS mode the TOE supports the following SSH data integrity algorithms:

i) HMAC-SHA1-96

ii) HMAC-SHA1

g) The TOE is configured to negotiate the above algorithms in order of preference. If a connecting client does not support the listed algorithms the connection will be refused.

#### 6.7.2.1 SSH Underlying Cryptography

180 The Gateway OS implements OpenSSL to provide the cryptographic primitives used by SSH. Table 21 identifies these components and related CAVP certificates. This implementation makes use of the CTR_DRBG(AES) seeded by the entropy source described in the supplementary Entropy Description.

**Table 21: OpenSSL/SSH CAVP Certificates**

| Algorithm | CAVP Certificate |
|---|---|
| AES | #4429 |
| SHA | #3647 |
| HMAC | #2941 |
| RSA | #2570 |
| CTR_DRBG | #1606 |

181 The TOE complies with NIST SP 800-56B as relevant to the use of RSA within SSH. The TOE implements all sections of SP 800-56B relevant to RSA key generation. The TOE does not perform any operation marked as “Shall Not” or “Should not” in SP 800-56B. Additionally, the TOE does not omit any operation marked as “Shall.”

## 6.8 Third-Party Cryptographic Modules

182 Gateway cryptographic operations, other than for SSH remote administrator connections, are performed by the CryptoComply software module unless a HSM is installed in which case the HSM will provide Gateway cryptographic functions (see section 2.3.2 for supported HSM).

183 All Policy Manager cryptographic operations are performed by the CryptoComply software module.

### 6.8.1 CryptoComply

184 The TOE invokes CryptoComply cryptographic functionality via Java API calls to the module.

185 CryptoComply is seeded by the underlying OS in the TOE environment as follows:

a) **Policy Manager.** Microsoft Crypto API.

b) **Gateway.** RHEL /dev/urandom (as described in the supplementary Entropry Description).

### 6.8.2 HSM (Thales nShield Solo+)

186 The TOE invokes HSM cryptographic functionality via Java API calls to the module.

187 The HSM internally generates cryptographic seeds using a hardware entropy source.

# 7 Rationale

## 7.1 Conformance Claim Rationale

188 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is an enterprise security management solution that provides centralized management and access control over web services. The Policy Manager is consistent with the TOE type identified by the ESM Policy Manager PP and the Gateway is consistent with the TOE type identified in the ESM Access Control PP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are identical to those of the ESM Policy Manager PP and the ESM Access Control PP**.**

c) **Security objectives.** As shown in section 4, the security objectives are identical to those of the ESM Policy Manager PP and the ESM Access Control PP.

d) **Security requirements.** Section 5 of this ST defines the claimed security requirements. SARs have been reproduced directly from the claimed PPs. There were a number of duplicate SFRs included in both the ESM Policy Manager PP and the ESM Access Control PP. Table 22 below describes how this duplication has been addressed. In addition, the claimed PPs included a number of optional SFRs, Table 23 below describes how these have been addressed. No additional requirements have been specified.

189 The conformance of this ST to both the ESM Policy Manager PP and the ESM Access Control PP is consistent with the PP application notes presented in section 6.1.1 of each document, which states: *'The ESM PPs represent a family of related Protection Profiles written to encompass the variable capabilities of ESM products. For an ST that claims conformance to multiple PPs within the ESM PP family, it is recommended that the ST author clarify how the ESM components relate to one another through usage of application notes. This will assist the reader in determining how the parts of the product that are to be evaluated correspond with the CC's notion of different ESM capabilities*.'

**Table 22: Duplicate SFRs**

| Requirement | How the duplication of SFRs is handled in the ST |
|---|---|
| ESM_EID.2 | Iteration. |
| FAU_GEN.1 | Same base requirement in both PPs. SFR specified once in the ST and events combined in Table 16. |
| FAU_STG_EXT.1 | SFR from the ESM Policy Manager PP included in the ST as it is a superset of the SFR defined by the ESM Access Control PP. |
| FCS_CKM.1 | SFRs from the ESM Access Control PP have been included to address cryptographic functions related to SSH remote administration. |
| FCS_CKM_EXT.4 | |
| FCS_COP.1(1) | |

| Requirement | How the duplication of SFRs is handled in the ST |
|---|---|
| FCS_COP.1(2) | |
| FCS_COP.1(3) | |
| FCS_COP.1(4) | |
| FCS_RBG_EXT.1 | |
| FCS_SSH_EXT.1 | Same requirement in both PPs. SFR specified once in the ST. |
| FCS_TLS_EXT.1 | Same requirement in both PPs. SFR specified once in the ST. |
| FMT_SMF.1 | Same base requirement in both PPs. SFR specified once in the ST and management functions combined in Table 17. |
| FMT_SMR.1 | Same requirement in both PPs. SFR specified once in the ST. |
| FPT_APW_EXT.1 | Same requirement in both PPs. SFR specified once in the ST. |
| FPT_SKP_EXT.1 | Same requirement in both PPs. SFR specified once in the ST. |
| FTA_TSE.1 | Not claimed (optional). |
| FTP_ITC.1 | Same requirement in both PPs. SFR specified once in the ST. |

**Table 23: Optional SFRs**

| Requirement | Source | Rationale |
|---|---|---|
| ESM_ATD.1 | ESM Policy Manager PP | Included |
| ESM_ATD.2 | ESM Policy Manager PP | Included |
| ESM_DSC.1 | ESM Access Control PP | Not included.<br>Per ESM Access Control PP section C.2, this SFR is relevant to Data Loss Prevention or similar TOEs that require automated discovery and inventory of objects. In the TOE, objects (Web Services) are manually added by the administrator. |
| FAU_SEL.1 | ESM Policy Manager PP | Not included. FAU_SEL_EXT.1 included. |
| FCS_CKM.1 | ESM Policy Manager PP<br>ESM Access Control PP | Included for SSH only.<br>The TOE utilizes third-party cryptographic suites for all other cryptographic functions - related guidance at Annex C.8 of the ESM Policy Manager PP and Annex C.5 of the |
| FCS_CKM_EXT.4 | | |
| FCS_COP.1(1) | | |

| Requirement | Source | Rationale |
|---|---|---|
| FCS_COP.1(2) | | Access Control PP. |
| FCS_COP.1(3) | | |
| FCS_COP.1(4) | | |
| FCS_RBG_EXT.1 | | |
| FCS_HTTPS_EXT.1 | ESM Policy Manager PP<br>ESM Access Control PP | Not included as the TOE does not provide these protocols. |
| FCS_IPSEC_EXT.1 | | |
| FIA_AFL.1 | ESM Policy Manager PP | Not included. The Policy Manager makes use of an external authentication server. A.ROBUST included. |
| FIA_SOS.1 | ESM Policy Manager PP | |
| FPT_FLS.1 | ESM Access Control PP | Not included.<br>Per ESM Access Control PP sections C.3, this SFR is relevant to systems that require continued enforcement mechanisms to counter the threat of disablement by users, such as host based access control systems. The TOE is not a host based access control system. |
| FPT_STM.1 | ESM Policy Manager PP | Included |
| FTA_SSL_EXT.1 | ESM Policy Manager PP | Included |
| FTA_SSL.3 | ESM Policy Manager PP | Not included. No remote access to the Policy Manager. |
| FTA_SSL.4 | ESM Policy Manager PP | Included |
| FTA_TSE.1 | ESM Policy Manager PP<br>ESM Access Control PP | Not included. Not required. |

## 7.2 Security Objectives Rationale

190 All security objectives are drawn directly from the ESM Policy Manager PP and the ESM Access Control PP. A conformance rationale is presented at section 7.1.

## 7.3 Security Requirements Rationale

191 Security requirements are drawn directly from the ESM Policy Manager PP and the ESM Access Control PP. A conformance rationale is presented at section 7.1.

192 Table 24 below presents the SFR dependency rationale based on the ESM Policy Manager PP and the ESM Access Control PP.

**Table 24: SFR Dependency Rationale**

| Requirement | Dependencies | Met / Rationale if not met |
|---|---|---|
| ESM_ACD.1 | None | - |
| ESM_ACT.1 | ESM_ACD.1 | Met |
| ESM_ATD.1 | None | - |
| ESM_ATD.2 | None | - |
| ESM_EAU.2 | ESM_EID.2 | Met |
| ESM_EID.2(1) | None | - |
| ESM_EID.2(2) | None | - |
| FAU_GEN.1 | FPT_STM.1 | Not met. This SFR is an unfulfilled dependency on FAU_GEN.1. It has not been included because the TOE is not necessarily expected to include its own system clock. The ST author must examine the entire ESM under evaluation in order to determine the point of origin for system time. If the evaluation boundary is an entire ESM appliance that uses an internal system clock, FPT_STM.1 must be claimed. However, if the ESM relies on an environmental component such as a host operating system or NTP server, it is an acceptable alternative to represent accurate system time as an environmental objective. |
| FAU_SEL.1 | FAU_GEN.1 | Met |
| | FMT_MTD.1 | Not met. It has not been included because the intent of the dependency is that the TSF data governing the configuration of the auditing function is expected to be configurable. This dependency is satisfied by FMT_MOF.1(1) because the auditing behavior is considered to be a function of the TSF rather than a collection of TSF data. |
| FAU_STG.1 | FAU_GEN.1 | Met |
| FAU_SEL_EXT.1 | FAU_GEN.1 | Met |

| Requirement | Dependencies | Met / Rationale if not met |
|---|---|---|
| | FMT_MTD.1 | Not met. It has not been included because the intent of the dependency is that the TSF data governing the configuration of the auditing function is expected to be configurable. This dependency is satisfied by FMT_MOF.1(1) because the auditing behavior is considered to be a function of the TSF rather than a collection of TSF data. |
| FAU_STG_EXT.1 | FAU_GEN.1 | Met |
| | FTP_ITC.1 | Met |
| FCO_NRR.2 | FIA_UID.1 | Not met. It has not been included because the application notes and defined assignments of FCO_NRR.2 state that the identity of policy origin is limited to software/hardware information rather than the user identity of any user initiating the policy forwarding function. |
| FCS_CKM.1 | FCS_CKM.2, or<br>FCS_COP.1 | Met |
| | FCS_CKM.4 | Met |
| FCS_CKM_EXT.4 | None | - |
| FCS_COP.1(1)<br>FCS_COP.1(2)<br>FCS_COP.1(3)<br>FCS_COP.1(4) | FDP_ITC.1, or<br>FDP_ITC.2, or<br>FCS_CKM.1 | Met |
| | FCS_CKM.4 | Met |
| FCS_RBG_EXT.1 | None | - |
| FCS_SSH_EXT.1 | FCS_COP.1 | Met |
| FCS_TLS_EXT.1 | FCS_COP.1 | Not met. The TOE utilizes third-party cryptographic modules for TLS cryptographic primitives and therefore does not claim FCS_CKM, FCS_COP or FCS_RBG_EXT for TLS per guidance at Annex C.8 of the ESM Policy Manager PP and Annex C.5 of the Access Control PP. |
| FDP_ACC.1 | FDP_ACF.1 | Met |
| FDP_ACF.1 | FDP_ACC.1 | Met |
| | FMT_MSA.3 | Met |

| Requirement | Dependencies | Met / Rationale if not met |
|---|---|---|
| FIA_USB.1 | FIA_ATD.1 | Not met. It has not been included because the ESM Policy Management product is expected to use user security attributes rather than define them. Any attributes that can be used to define policies should already be defined by a compatible Identity and Credential Management product; if not, they may be defined by the ESM_ATD components. |
| FMT_MOF.1<br>FMT_MOF.1(1)<br>FMT_MOF.1(2)<br>FMT_MOF_EXT.1 | FMT_SMF.1 | Met |
| | FMT_SMR.1 | Met |
| FMT_MSA.1 | FDP_ACC.1, or FDP_IFC.1 | Met |
| | FMT_SMF.1 | Met |
| | FMT_SMR.1 | Met |
| FMT_MSA.3 | FMT_MSA.1 | Met |
| | FMT_SMR.1 | Met |
| FMT_MSA_EXT.5 | FMT_MOF_EXT.1 | Met |
| FMT_SMF.1 | None | - |
| FMT_SMR.1 | FIA_UID.1 | Not met. ESM_EID.2 satisfies this dependency by providing equivalent functionality. |
| FPT_APW_EXT.1 | None | - |
| FPT_FLS_EXT.1 | None | - |
| FPT_RPL.1 | None | - |
| FPT_SKP_EXT.1 | None | - |
| FRU_FLT.1 | FPT_FLS.1 | Not met. This dependency is satisfied through the alternate explicit requirement FPT_FLS_EXT.1. |
| FTA_SSL_EXT.1 | None | - |
| FTA_SSL.4 | None | - |
| FTA_TAB.1 | None | - |
| FTP_ITC.1 | None | - |

| Requirement | Dependencies | Met / Rationale if not met |
|---|---|---|
| FTP_TRP.1 | None | - |

## 7.4 TOE Summary Specification Rationale

193 Table 25 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

**Table 25: Map of SFRs to TSS Security Functions**

| SFR | Access Control Policy Definition | Access Control Policy Enforcement | Policy Security | System Monitoring | Secure Administration | Continuity of Enforcement |
|---|---|---|---|---|---|---|
| ESM_ACD.1 | X | | | | | |
| ESM_ACT.1 | | | X | | | |
| ESM_ATD.1 | X | | | | | |
| ESM_ATD.2 | X | | | | | |
| ESM_EAU.2 | | | | | X | |
| ESM_EID.2(1) | | | | | X | |
| ESM_EID.2(2) | | X | | | | |
| FAU_GEN.1 | | | | X | | |
| FAU_SEL.1 | | | | X | | |
| FAU_STG.1 | | | | X | | |
| FAU_SEL_EXT.1 | | | | X | | |
| FAU_STG_EXT.1 | | | | X | | |
| FCO_NRR.2 | | | X | | | |
| FCS_CKM_EXT.4 | | | | | X | |
| FCS_COP.1(1) | | | | | X | |
| FCS_COP.1(2) | | | | | X | |
| FCS_COP.1(3) | | | | | X | |

| SFR | Access Control Policy Definition | Access Control Policy Enforcement | Policy Security | System Monitoring | Secure Administration | Continuity of Enforcement |
|---|---|---|---|---|---|---|
| FCS_COP.1(4) | | | | | X | |
| FCS_RBG_EXT.1 | | | | | X | |
| FCS_SSH_EXT.1 | | | | | X | |
| FCS_TLS_EXT.1 | | X | X | X | | |
| FDP_ACC.1 | | X | | | | |
| FDP_ACF.1 | | X | | | | |
| FIA_USB.1 | | | | | X | |
| FMT_MOF.1 | X | | | | | |
| FMT_MOF.1(1) | | X | | | | |
| FMT_MOF.1(2) | | X | | | | |
| FMT_MOF_EXT.1 | | X | | | | |
| FMT_MSA.1 | | X | | | | |
| FMT_MSA.3 | | X | | | | |
| FMT_MSA_EXT.5 | X | | | | | |
| FMT_SMF.1 | X | X | | | | |
| FMT_SMR.1 | | X | | | X | |
| FPT_APW_EXT.1 | | | | | X | |
| FPT_FLS_EXT.1 | | | | | | X |
| FPT_RPL.1 | | | X | | | |
| FPT_SKP_EXT.1 | | | | | X | |
| FRU_FLT.1 | | | | | | X |
| FTA_SSL_EXT.1 | | | | | X | |

| SFR | Access Control Policy Definition | Access Control Policy Enforcement | Policy Security | System Monitoring | Secure Administration | Continuity of Enforcement |
|---|---|---|---|---|---|---|
| FTA_SSL.4 | | | | | X | |
| FTA_TAB.1 | | | | | X | |
| FTP_ITC.1 | | X | X | X | | |
| FTP_TRP.1 | | | | | X | |

# Annex A: Access Control Matrix

| Ref. | Management Function | Role (permission if restricted) |
|---|---|---|
| FMT_SMF.1 | Configuration of audited events | Administrator<br>Operator (Read) |
| FMT_SMF.1 | Configuration of repository for trusted audit storage | Administrator<br>Manage Log Sinks<br>Operator (Read) |
| FMT_SMF.1 | Configuration of Access Control SFP | Administrator<br>Manage [name] Folder (limited to policies within a defined folder)<br>Manage[name] Policy (limited to the named policy)<br>Manage [name] Service (limited to assertions for a defined web service)<br>Manage Web Services (Global Policies and assertions for web service policies)<br>Operator (Read) |
| FMT_SMF.1 | Querying of policy being implemented by the TSF | Administrator<br>Operator (Read) |
| FMT_SMF.1 | Management of Access Control SFP behavior to enforce in the event of communications outage | Not Configurable |
| ESM_ACD.1 | Creation of policies | Administrator<br>Manage [name] Folder (limited to policies within a defined folder)<br>Manage [name] Service (limited to assertions for a defined web service)<br>Manage Web Services (Global Policies and assertions for web service policies)<br>Operator (Read) |

| Ref. | Management Function | Role (permission if restricted) |
|---|---|---|
| ESM_ACT.1 | Transmission of policies | Administrator<br>Manage [name] Folder (limited to policies within a defined folder)<br>Manage[name] Policy (limited to the named policy)<br>Manage [name] Service (limited to assertions for a defined web service) |
| ESM_ATD.1 | Definition of object attributes.<br>Association of attributes with objects. | Administrator<br>Manage [name] Folder (limited to policies within a defined folder)<br>Manage[name] Policy (limited to the named policy)<br>Manage [name] Service (limited to assertions for a defined web service)<br>Manage Web Services (assertions for web service policies)<br>Publish Web Services |
| ESM_ATD.2 | Definition of subject attributes.<br>Association of attributes with subjects. | Administrator |
| ESM_EAU.2 | Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF) | Not managed by the TSF |
| ESM_EID.2 | Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF) | Not managed by the TSF |
| FAU_SEL.1 | Configuration of auditable events | Administrator<br>Operator (Read) |
| FAU_SEL_EXT.1 | Configuration of auditable events for defined external entities | Administrator<br>Operator (Read) |
| FAU_STG_EXT.1 | Configuration of external audit storage location | Administrator<br>Manage Log Sinks<br>Operator (Read) |

| Ref. | Management Function | Role (permission if restricted) |
|---|---|---|
| FIA_USB.1 | Definition of default subject security attributes, modification of subject security attributes | Administrator<br>Operator (Read) |
| FMT_MOF_EXT.1 | Configuration of the behavior of other ESM products | Administrator<br>Operator (Read) |
| FMT_MSA_EXT.5 | Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected | Not configurable |
| FMT_SMR.1 | Management of the users that belong to a particular role | Administrator<br>Manage Internal Users and Groups<br>Search Users and Groups (Read)<br>Operator (Read) |
| FTA_TAB.1 | Maintenance of the banner | Administrator<br>Operator (Read) |
| FTP_ITC.1 | Configuration of actions that require trusted channel | Administrator<br>Operator (Read) |
| FTP_TRP.1 | Configuration of actions that require trusted path | Administrator<br>Operator (Read) |