



**Imprivata
OneSign Version 7.9
Security Target**

Version:	1.3
Status:	Released
Last Update:	2023-10-06
Classification:	Public

Trademarks

The following term is a trademark of atsec information security corporation in the United States and/or other countries.

- atsec®

The following terms are trademarks or registered trademarks of The Apache Software Foundation in the United States and/or other countries.

- Apache®
- Apache HTTP Server
- Apache MINA
- Apache SSHD
- Apache Tomcat®
- MINA
- Tomcat®

The following terms are trademarks or registered trademarks of Dell Inc. in the United States and/or other countries.

- PowerEdge

The Imprivata logo is a trademark or registered trademark of Imprivata, Inc. in the United States and/or other countries. The following terms are also trademarks or registered trademarks of Imprivata, Inc. in the United States and/or other countries.

- Imprivata®
- OneSign®

The following terms are trademarks or registered trademarks of Intel Corporation in the United States and/or other countries.

- Intel®
- Xeon®

The following terms are trademarks or registered trademarks of Legion of the Bouncy Castle Inc. in the United States and/or other countries.

- Bouncy Castle Crypto API

The following terms are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

- Windows®
- Windows 10

The following terms are trademarks or registered trademarks of One Identity LLC in the United States and/or other countries.

- syslog-ng

The following terms are trademarks or registered trademarks of OpenSSL Software Foundation in the United States and/or other countries.

- OpenSSL®

The following terms are trademarks or registered trademarks of Oracle Corporation in the United States and/or other countries.

- Java®
- OpenJDK
- Oracle®

The following terms are trademarks or registered trademarks of SUSE LLC in the United States and/or other countries.

- SLES
- SUSE®

The following terms are trademarks or registered trademarks of VMware, Inc. in the United States and/or other countries.

- VMware
- VMware ESXi

Other company, product, and service names may be trademarks or service marks of others.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
1.0	2023-07-31	atsec	Final.
1.1	2023-09-12	atsec	Address ECRs
1.2	2023-09-26	atsec	Address ECRs. Remove cryptographic algorithms and key sizes not used by the SSH and TLS protocols.
1.3	2023-10-06	atsec	Add TD0794

Table of Contents

1	Introduction	8
1.1	Security Target Identification	8
1.2	TOE Identification	8
1.3	TOE Type	8
1.4	TOE Overview	8
1.4.1	Required non-TOE hardware and software	9
1.4.2	Intended method of use	9
1.4.3	Major security features	9
1.5	TOE Description	10
1.5.1	Introduction	10
1.5.2	Security functionality	11
1.5.3	TOE boundaries	16
2	CC Conformance Claim	18
2.1	Protection Profile Tailoring and Additions	18
3	Security Problem Definition	19
3.1	Threat Environment	19
3.1.1	Threats countered by the TOE	19
3.2	Assumptions	19
3.2.1	Environment of use of the TOE	19
3.3	Organizational Security Policies	20
4	Security Objectives	21
4.1	Objectives for the TOE	21
4.2	Objectives for the Operational Environment	22
4.3	Security Objectives Rationale	22
5	Extended Components Definition	23
6	Security Requirements	24
6.1	TOE Security Functional Requirements	24
6.1.1	(ESM)	26
6.1.2	Security audit (FAU)	28
6.1.3	Cryptographic support (FCS)	31
6.1.4	Identification and authentication (FIA)	34
6.1.5	Security management (FMT)	35
6.1.6	Protection of the TSF (FPT)	38
6.1.7	TOE access (FTA)	38
6.1.8	Trusted path/channels (FTP)	39
6.2	Security Functional Requirements Rationale	40
6.3	Security Assurance Requirements	40
6.4	Security Assurance Requirements Rationale	40
7	TOE Summary Specification	41
7.1	TOE Security Functionality	41
7.1.1	ESM_ACD.1 Access control policy definition	41

7.1.2	ESM_ACT.1 Access control policy transmission	42
7.1.3	ESM_ATD.1 Object attribute definition	43
7.1.4	ESM_ATD.2 Subject attribute definition	43
7.1.5	ESM_EAU.2 Reliance on enterprise authentication	43
7.1.6	ESM_EID.2 Reliance on enterprise identification	43
7.1.7	FAU_GEN.1 Audit data generation	43
7.1.8	FAU_SEL.1 Selective audit	44
7.1.9	FAU_SEL_EXT.1 External selective audit	44
7.1.10	FAU_STG_EXT.1 External audit trail storage	44
7.1.11	FCS_CKM.1 Cryptographic key generation (for asymmetric keys)	45
7.1.12	FCS_CKM_EXT.4 Cryptographic key zeroization	45
7.1.13	FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)	47
7.1.14	FCS_COP.1(2) Cryptographic operation (for cryptographic signature)	47
7.1.15	FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)	48
7.1.16	FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)	49
7.1.17	FCS_HTTPS_EXT.1 HTTPS	49
7.1.18	FCS_RBG_EXT.1 Cryptographic operation (random bit generation)	50
7.1.19	FCS_SSH_EXT.1 SSH	50
7.1.20	FCS_TLS_EXT.1(C) TLS client (syslog-ng)	51
7.1.21	FCS_TLS_EXT.1(S) HTTPS server	52
7.1.22	FIA_AFL.1 Authentication failure handling	52
7.1.23	FIA_USB.1 User-subject binding	53
7.1.24	FMT_MOF.1 Management of security functions behavior	53
7.1.25	FMT_MOF_EXT.1 External management of functions behavior	53
7.1.26	FMT_MSA_EXT.5 Consistent security attributes	55
7.1.27	FMT_SMF.1 Specification of management functions	55
7.1.28	FMT_SMR.1 Security roles	59
7.1.29	FPT_APW_EXT.1 Protection of stored credentials	60
7.1.30	FPT_SKP_EXT.1 Protection of secret key parameters	60
7.1.31	FPT_STM.1 Reliable time stamps	60
7.1.32	FTA_SSL.3 TSF-initiated termination	61
7.1.33	FTA_SSL.4 User-initiated termination	61
7.1.34	FTA_TAB.1 Default TOE access banners	61
7.1.35	FTA_TSE.1 TOE session establishment	61
7.1.36	FTP_ITC.1 Inter-TSF trusted channel	61
7.1.37	FTP_TRP.1 Trusted path	62
8	Abbreviations, Terminology, and References	63
8.1	Abbreviations	63
8.2	Terminology	66
8.3	References	67
A	Appendixes	71
A.1	Product Computer Policy	71
A.2	Product User Policy	78

List of Tables

Table 1: Operational environment hardware and software	9
Table 2: Appliance cryptographic providers	14
Table 3: Appliance secure protocols	16
Table 4: NIAP TDs for ESM PM PP	18
Table 5: SFRs for the TOE	24
Table 6: Computer Policy	26
Table 7: User Policy	27
Table 8: Combined Computer Policy and User Policy	27
Table 9: Auditable events	29
Table 10: Management functions	36
Table 11: TOE session establishment	39
Table 12: SARs	40
Table 13: Audit storage mechanisms	44
Table 14: Asymmetric key generation, verification, and establishment algorithms	45
Table 15: Key destruction	46
Table 16: Symmetric encryption/decryption algorithms	47
Table 17: Signature generation/verification algorithms	48
Table 18: Hash algorithms	48
Table 19: Keyed-hash message authentication algorithms	49
Table 20: DRBG algorithms	50
Table 21: Security management functions	55

List of Figures

Figure 1: Overview 10

1 Introduction

1.1 Security Target Identification

Title:	Imprivata OneSign Version 7.9 Security Target
Version:	1.3
Status:	Released
Date:	2023-10-06
Sponsor:	Imprivata, Inc.
Developer:	Imprivata, Inc.
Validation Body:	NIAP
Validation ID:	VID11178
Keywords:	Imprivata, OneSign, Single sign-on, SSO

1.2 TOE Identification

The TOE is Imprivata OneSign Version 7.9 Hot Fix 9 (HF9) (build 7.9.009.58).

1.3 TOE Type

The TOE type is enterprise security management (ESM) policy management (PM) software.

1.4 TOE Overview

OneSign is a policy management product developed by Imprivata, Inc. for managing endpoints in an enterprise. It manages access to endpoint features through the use of policies and provides single sign-on (SSO) capabilities for endpoints. The product consists of two main components:

1. **Imprivata Appliance**—A virtual appliance (a.k.a. appliance) containing software called OneSign that performs policy management (i.e., the TOE)
2. Imprivata Agent—Agent software (a.k.a. agent) for enforcing policies on endpoints

The TOE is the **Imprivata Appliance**.

The Imprivata Agents and endpoints reside in the operational environment.

The TOE is a single virtual appliance instance running in a VMware ESXi virtual machine. The TOE contains the SUSE Linux Enterprise Server (SLES) OS as its base OS, an Apache HTTP Server, Apache SSHD using Apache Multipurpose Infrastructure for Network Applications (MINA), Java, OpenJDK, and syslog-ng.

In ESM Protection Profile terms, the TOE is a Policy Manager. The Access Control products are the agents located on each endpoint. The TOE is used to create, manage, and provide policies to the enrolled endpoints. The agents enforce the policies on the endpoints.

For brevity, whenever the ST says endpoint, it means an endpoint with the Imprivata Agent installed and running, unless otherwise stated.

1.4.1 Required non-TOE hardware and software

The TOE requires hardware and other software components in order to operate. The hardware and other software components are part of the operational environment.

Table 1: Operational environment hardware and software

Component	Hardware/Software
Appliance	VMware ESXi 6.7 Update 3
	Dell PowerEdge R740xd 2U Rack Server with Intel Xeon Gold 5222 (Cascade Lake)
Agent	Imprivata Agent version 7.3
	Microsoft Windows 10 OS
Web browser	Administrative computer supporting at least one of the following web browsers: <ul style="list-style-type: none"> • Chrome • Microsoft Edge Chromium

1.4.2 Intended method of use

The TOE is intended to be used in a non-hostile environment inside of an enterprise and located in a protected environment (e.g., server room) where only trusted administrators have access to the physical computer.

The Imprivata Agent software is intended to be installed on Windows 10 OS computer systems inside of the enterprise.

1.4.3 Major security features

The TOE supports the following major security features:

- Enterprise security management (ESM)
- Auditing (FAU)
- Cryptographic support (FCS)
- Identification and authentication (FIA)
- Security management (FMT)
- Protection of the TOE security functionality (FPT)
- TOE access (FTA)
- Trusted path/channels (FTP)

1.5 TOE Description

1.5.1 Introduction

The TOE is a virtual appliance that provides policy management for agents deployed on endpoints in the enterprise. Thus, the use of the terms "TOE" and "appliance" in this Security Target (ST) are synonymous. The agents and the endpoints that the agents run on are both in the operational environment.

Figure 1 provides an overview of the TOE, TOE boundary, Admin Console, Appliance Console, external audit logging devices, and agents. It also shows the TOE as a closed, self-contained system with protected communication paths.

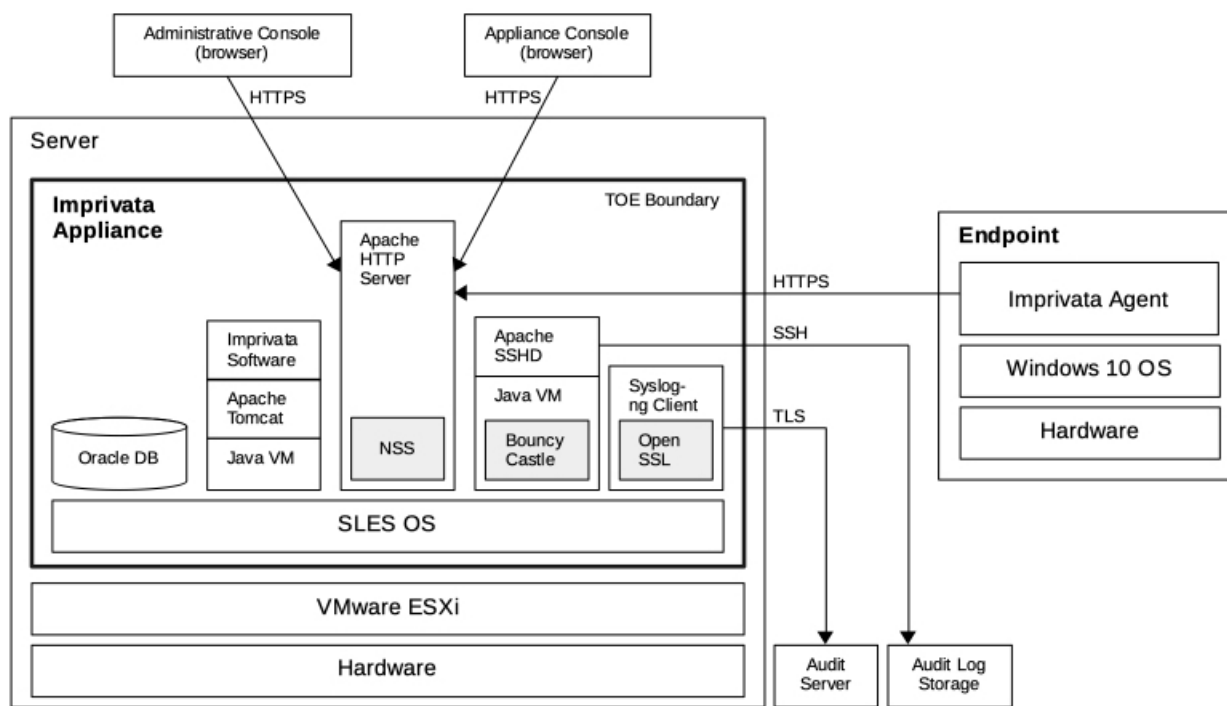


Figure 1: Overview

Figure 1 shows the TOE as a virtual appliance inside a VMware ESXi container. The TOE contains the following components:

- Imprivata software—Used to perform policy management.
- Apache Tomcat v9.0.36—Used to support Imprivata's software.
- Apache HTTP Server v2.4.51—Used as the appliance's HTTPS server for all HTTPS communications. It supports PHP 7.4.6. Apache HTTP Server uses the Apache Network Security Services (Apache NSS v3.77) cryptographic module for the TLS protocol's cryptographic module.
- Apache SSHD v2.4.0—A secure shell (SSH) client used to copy appliance audit logs to external audit log storage. Apache SSHD requires Apache MINA, which runs in a Java virtual machine (VM) and uses Bouncy Castle v1.68 for the SSH protocol's cryptographic module.

- syslog-ng v3.35—A syslog client used to copy audit records to an external audit server (syslog server) over TLS. syslog-ng uses OpenSSL v1.0.2p for the transport layer security (TLS) protocol's cryptographic module.
- Oracle Database 19—Used to store user accounts, user authentication data, policies, and audit data.
- Java VM 17 (a.k.a. v1.17)—Used to support multiple TOE products.
- SLES 12 SP5 (Linux kernel version 4.12.14)—Used as the OS.

The figure shows two web browser interfaces in the operational environment used to administer the TOE:

- Admin Console
- Appliance Console

Both web browsers connect to the TOE's Apache HTTP Server over HTTPS connections.

The figure also shows an endpoint containing the Imprivata Agent. A normal deployment contains thousands of endpoints each with an installed agent. In the evaluated configuration, the agents are installed and run on Windows 10 OS. Agents contact the TOE's Apache HTTP Server over an HTTPS connection. The figure shows the entire endpoint, including the agent and Windows 10 OS, as part of the operational environment.

In addition, the figure shows the TOE connecting to two external audit logging devices in the operational environment:

- Audit server
- Audit log storage

These devices are used to fulfill the external audit trail storage requirements of the protection profile. Both connections use a protected communications channel (TLS and SSH, respectively).

Not shown in the figure is the TOE's internal authentication server. This authentication server is used by the TOE to authenticate both the Admin Console users and endpoint users. The product also supports external authentication servers (e.g., Microsoft Active Directory (AD)). In the evaluated configuration, only the internal authentication server was configured and tested.

The Appliance Console is a low-use administrative interface, used only for low-level configuration. It is included in the TOE because it fulfills one or more security management functions required by [ESMPMPP]. The Appliance Console uses an internal password file for identification and authentication.

1.5.2 Security functionality

The TOE supports the following security functionality.

- Enterprise security management (ESM)
- Auditing (FAU)
- Cryptographic support (FCS)
- Identification and authentication (FIA)
- Security management (FMT)
- Protection of the TOE security functionality (FPT)
- TOE access (FTA)
- Trusted path/channels (FTP)

1.5.2.1 TOE security functionality

1.5.2.1.1 Enterprise security management

The TOE supports policy definition and transmission. It allows administrators to define security policies and distribute the policies over a secure connection to the managed endpoints.

The TOE supports the following policies:

- Computer Policy—Capabilities and restrictions placed on the endpoint
- User Policy—Capabilities and restrictions placed on the user

The agent combines and enforces the two policies when a user authenticates to an endpoint.

1.5.2.1.1.1 Computer policy

In general, Computer Policies apply to every user attempting to use the endpoint. These policies define the set of features accessible to any user on that endpoint.

The TOE supports the creation (including modification and deletion) of multiple Computer Policies and the application of different Computer Policies to different endpoints. This allows for different Computer Policies to be assigned to different endpoints at any given time.

Computer Policies can control many endpoint features such as the types of allowed authentication methods (e.g., passwords, proximity cards, fingerprints), inactivity lockouts, and virtual desktops (e.g., Citrix, VMware). The full Computer Policy is provided in [Appendix A.1](#).

The evaluated configuration only tests the following Computer Policy items. (Many items in the policy have editable fields that allow an administrator to configure the policy. These editable fields contain the terms: "select", "assignment", and "edit".)

- General
 - Shutdown/restart workstation from lock screen (Select one of: Enable, Disable)
- Walk-Away Security
 - Inactivity detection
 - Keyboard and mouse
 - Lock workstation after (Assignment: Specify time in minutes)
- Override and Restrict
 - Desktop Access Authentication Restrictions
 - Restrict user policy (Select one of: Enable, Disable)
 - Primary factors
 - Password (Select one of: Enable, Disable)

When an agent contacts the TOE for the first time, the TOE automatically assigns a default Computer Policy to that endpoint without administrator intervention. An administrator can later assign a different policy to that endpoint. An administrator can also modify the default Computer Policy to be more restrictive or more permissive.

1.5.2.1.1.2 User Policy

In general, User Policies apply to a specific user attempting to use any endpoint. These policies define the set of endpoint features the user is allowed to use on any endpoint, assuming the endpoint's Computer Policy allows it and the endpoint supports the feature.

The TOE supports the creation (including modification and deletion) of multiple User Policies and the application of different User Policies to different users. This allows for different User Policies to be assigned to different users at any given time.

User Policies can control user access to many endpoint features such as the types of allowed authentication methods (e.g., passwords, proximity cards, fingerprints), inactivity lockouts, and virtual desktops (e.g., Citrix, VMware). The full User Policy is provided in [Appendix A.2](#).

The evaluated configuration only tests the following User Policy items. (Many items in the policy have editable fields that allow an administrator to configure the policy. These editable fields contain the terms: "select", "assignment", and "edit".)

- Authentication
 - Primary factors
 - Password (Select one of: Enable, Disable)
 - Lockout
 - Lock user account after (Assignment: Specify number of failed attempts) consecutive failures within (Assignment: Specify time in minutes) minutes
 - Lock account for (Assignment: Specify time in minutes) minutes

A user policy is assigned to a user by the administrator when the user is initially created. The administrator can later assign a different policy to the user.

1.5.2.1.1.3 Using the policies

It is the agent's responsibility to interpret and enforce the two types of policies. In the areas where the two policies intersect, such as in the area of authentication mechanisms, the agent only uses the features that both policies allow.

For example, if the User Policy only allows password-based authentication and the Computer Policy only allows fingerprint authentication, then the agent will not allow the user to log on to that endpoint.

1.5.2.1.2 Auditing

The TOE generates audit records for the PP-required events. An administrator can select events to be audited by the TOE based on the event type. The records are protected from unauthorized modification and deletion within the TOE.

The TOE supports two separate mechanisms for storing its audit records externally. Some audit records can be transmitted as individual audit records to an external audit server (a.k.a. syslog server) over a protected communications channel. The remaining audit records can be transmitted in log files to external audit log storage over a protected communications channel.

The TOE allows an administrator to select the events audited by the agent based on event type.

1.5.2.1.3 Cryptographic support

The TOE employs the HTTPS protocol, SSH (a.k.a. SSHv2) protocol, and TLS protocol to protect communication channels.

The HTTPS protocol is implemented by the Apache HTTP Server. The Apache HTTP Server uses Apache's Network Security Services (NSS) for its TLS implementation. Apache NSS is a software module that implements both the TLS protocol and cryptographic algorithms.

The SSH protocol is implemented using Apache SSHD. Apache SSHD requires Apache MINA, which requires the Java Virtual Machine (VM). The Java VM uses a Bouncy Castle software cryptographic module as the cryptographic provider for the Java Secure Socket Extension (JSSE). Apache SSHD uses the JSSE application programming interface (API) to perform its cryptographic operations in the SSH protocol.

The syslog-ng client uses OpenSSL for its TLS implementation. OpenSSL is a software module that implements both the TLS protocol and cryptographic algorithms.

Table 2: Appliance cryptographic providers

Cryptographic provider	Protocol	Usage
Apache NSS v3.77	HTTPS (TLS 1.2)	Apache HTTP Server
Bouncy Castle v1.68	SSHv2	Java VM (Apache SSHD)
OpenSSL v1.0.2p	TLS 1.2	syslog-ng

1.5.2.1.4 Identification and authentication

Admin Console

For the Admin Console, the TOE contains an internal authentication server used to authenticate users. The authentication server uses an internal database to store user data and credentials. The TOE requires the Admin Console users to be identified and authenticated prior to accessing any management functions.

The TOE enforces authentication failure handling on the Admin Console.

The Admin Console supports multiple administrator roles. Administrator roles consist of zero or more administrator role attributes. Multiple administrator roles can be assigned to an administrator. The administrator role attributes of these roles are summed together when the user logs in to the Admin Console to provide the administrator with a complete set of administrator role attributes. More information about administrator roles is provided in [section 1.5.2.1.5](#).

Appliance Console

For the Appliance Console, the TOE uses a separate password file to store and authenticate users. The TOE also enforces authentication failure handling on the Appliance Console.

The Appliance Console supports two administrator accounts: Super Administrator and Administrator. These accounts are used to perform low-level configuration and maintenance.

1.5.2.1.5 Security management

The TOE supports multiple security management functions required by the PP. These include user account management and policy management functions. The set of management functions is described in the TSS.

The Admin Console supports two types of administrator roles:

- Super Administrator
- Delegated Administrator

The Super Administrator can perform all administrative functions supported by the Admin Console. A Delegated Administrator can only perform functions delegated to it through the use of administrator role attributes.

The Appliance Console supports the following roles:

- Super Administrator
- Administrator

The Administrator role provides access to a subset of the functionality of the Super Administrator role.

[Section 7.1.28](#) provides more details on the above Admin Console and Appliance Console roles.

Agents must periodically contact the TOE to receive updated policies and information. The frequency at which the agents contact the TOE is called the Refresh Interval. The Refresh Interval is a global value managed by administrators through the TOE's Admin Console with a value ranging from 3 minutes to 24 hours.

In the OneSign architecture, the TOE never contacts the agents. Instead, the agents contact the TOE under the following conditions:

- At each agent Refresh Interval
- Each time a user attempts to authenticate to an endpoint/agent

1.5.2.1.6 Protection of the TSF

The TOE obscures authentication data before storing them in non-volatile memory. No interface is provided by the TOE to view the passwords in plaintext. Similarly, the TOE provides no interface to view pre-shared keys, symmetric keys, and private keys.

The TOE also provides its own reliable time stamp capabilities.

1.5.2.1.7 TOE access

The TOE terminates the remote sessions of the Admin Console and Appliance Console after an administrator-configurable time interval of inactivity. It also allows administrators to terminate their own sessions on the Admin Console and Appliance Console (i.e., logout).

The Admin Console and Appliance Console display configurable advisory messages prior to authentication. Depending on which console, administrators can deny session establishment based on day, time, duration, or username.

1.5.2.1.8 Trusted path/channels

The TOE acts as an HTTPS server supporting TLS 1.2 when communicating with the agents. Administrators externally manage the TOE using a web browser (i.e., Admin Console and Appliance Console) over HTTPS with TLS 1.2.

The TOE uses the secure copy protocol (SCP) (i.e., SSHv2) to protect the communication channel when transferring audit data from the TOE to external audit log storage.

The TOE uses TLS 1.2 to protect the communication channel when transferring audit data from the TOE to the external audit server (syslog).

Table 3: Appliance secure protocols

Protocol	Initiator
HTTPS (TLS 1.2)	Admin Console to TOE
	Appliance Console to TOE
	Agent to TOE
SSHv2 client	TOE to External audit log storage
TLS 1.2	TOE to External audit server (syslog)

1.5.3 TOE boundaries

1.5.3.1 Physical

The TOE is software and guidance only and is available as a download via the Imprivata website after purchase.

The TOE software (OneSign build 7.9.009.58) consists of the following images:

- 7.9_PROD_G4_OVF.rar
- virtual-applianceG4-IMPRIVATA-2023-2-1.ipm
- virtual-imprivataG4-7-9-9.ipm
- enableAccessControlNIAP-2022-9-12.ipm
- increasePHPmaxPOST-2021-1-22.ipm

The TOE administrative guidance document is the following:

- Imprivata OneSign Version 7.9 Common Criteria Administration Guide

The agent, which is part of the operational environment, is contained in the following download image:

- ImprivataAgent_x64.msi

1.5.3.2 Logical

The TOE's logical boundary is the virtual appliance shown in [Figure 1](#). The logical boundary contains the security functionality defined in [section 1.5.2](#).

1.5.3.3 Evaluated configuration

The following configuration specifics apply to the evaluated configuration of the TOE:

- The TOE is a single virtual appliance instance.
- Offline Authentication mode is disabled in the Computer Policies and User Policies.
- Only the internal password authentication mechanism is supported (i.e., external authentication servers were not tested).
- Only users in the Imprivata domain are supported.
- *Temporary Codes for Windows Access* are disallowed.
- Apache HTTP Server TLS 1.3 support is disabled.
- Network Time Protocol (NTP) is disabled.
- File servers for backup functionality are disallowed.
- Computer Policy settings:
 - General » Authentication » "Allow Users to Exit and Disable Agent" is disabled.
 - General » Authentication » "Kerberos authentication in place of OneSign authentication" is disabled.
 - General » Authentication » "If OneSign authentication fails, but Windows authentication succeeds, should the user be allowed to log in to the computer?" is set to No.
 - "Override and Restrict" » "Desktop Access Authentication Restrictions" » "Allow offline authentication" is disabled.
- User Policy settings:
 - "Desktop Access authentication" » "Allow offline authentication" is disabled.
- The following features were not tested:
 - Fingerprint, Proximity Card, Security Key, Smart Card, USB token, ID token, VASCO OTP, Security Questions, Remote access authentication, OneSign Anywhere authentication, Imprivata ID, Imprivata PIN, Spine Combined Workflow sessions, Self-Service Password, Imprivata Confirm ID, Virtual Desktops, Extensions, Citrix XenApp, Terminal Server, Fast User Switching, ProveID

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL1.

This Security Target claims conformance to the following Protection Profiles and PP packages:

- [ESMPMPP][\[1\]](#): Standard Protection Profile for Enterprise Security Management Policy Management. Version 2.1 as of 2013-10-24; exact conformance.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

2.1 Protection Profile Tailoring and Additions

This ST claims exact conformance to [ESMPMPP][\[1\]](#). This claim satisfies the requirement of strict conformance described in section 2.4 of the [ESMPMPP][\[1\]](#) as well as the requirement of exact conformance described in NIAP Policy Letter #1 [CCEVS-PL01][\[1\]](#).

Table 4 contains the NIAP TDs for this protection profile at the time of the evaluation and a statement of applicability to the evaluation.

Table 4: NIAP TDs for ESM PM PP

NIAP TD	TD description	Applicable?	Non-applicability rationale	TD reference
TD0794	Correction to FCS_SSH_EXT.1.7 Test 2	Yes		[CCEVS-TD0794] [1]
TD0621	Corrections to FCS_TLS_EXT.1 in ESM PPs	Yes		[CCEVS-TD0621] [1]
TD0576	FTP_ITC and FTP_TRP Updated	Yes		[CCEVS-TD0576] [1]
TD0574	Update to FCS_SSH in ESM PPs	Yes		[CCEVS-TD0574] [1]
TD0573	Update to FCS_COP and FCS_CKM in ESM PPs	Yes		[CCEVS-TD0573] [1]
TD0079	RBG Cryptographic Transitions per NIST SP 800-131A Revision 1	Yes		[CCEVS-TD0079] [1]
TD0066	Clarification of FAU_STG_EXT.1 Requirement in ESM PPs	Yes		[CCEVS-TD0066] [1]
TD0055	Move FTA_TAB.1 to Selection-Based Requirement	Yes		[CCEVS-TD0055] [1]
TD0042	Removal of Low-level Crypto Failure Audit from PPs	Yes		[CCEVS-TD0042] [1]

3 Security Problem Definition

3.1 Threat Environment

The threat environment is provided by the PPs to which this ST conforms.

3.1.1 Threats countered by the TOE

T.ADMIN_ERROR

An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

T.CONTRADICT

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.

3.2 Assumptions

The assumptions are provided by the PPs to which this ST conforms.

3.2.1 Environment of use of the TOE

A.ESM

The TOE will be able to establish connectivity to other ESM products in order to share security data.

A.MANAGE

There will be one or more competent individuals assigned to install, configure, and operate the TOE.

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.USERID

The TOE will receive validated identity data from the Operational Environment.

3.3 Organizational Security Policies

The organizational security policies are provided by the PPs to which this ST conforms.

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.

4 Security Objectives

The security objectives are provided by the PPs to which this ST conforms.

4.1 Objectives for the TOE

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.CRYPTO

The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.

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.

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 for administrators, other parts of a distributed TOE, and authorized IT entities.

O.ROBUST

The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.

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.

4.2 Objectives for the Operational Environment

OE.ADMIN

There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.

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.USERID

The Operational Environment shall be able to identify a user requesting access to the TOE.

4.3 Security Objectives Rationale

Any security objectives rationale is provided by the PPs to which this ST conforms.

5 Extended Components Definition

Extended components definitions (ECDs) are provided by the PPs to which this ST conforms. [Section 2](#) contains the list of PPs.

6 Security Requirements

6.1 TOE Security Functional Requirements

The table below summarizes the SFRs for the TOE and the operations performed on the components according to CC part 1. Operations in the SFRs use the following convention:

- Iterations (Iter.) are identified by appending a suffix to the original SFR.
- Refinements (Ref.) added to the text are shown in *italic text*, deletions are shown as ~~strikethrough text~~.
- Assignments (Ass.) are shown in **bold text**.
- Selections (Sel.) are shown in **bold text**.

Table 5: SFRs for the TOE

Security functional class	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
ESM -	ESM_ACD.1 Access control policy definition		ESMPMPP	No	No	Yes	No
	ESM_ACT.1 Access control policy transmission		ESMPMPP	No	No	Yes	Yes
	ESM_ATD.1 Object attribute definition		ESMPMPP	No	No	Yes	No
	ESM_ATD.2 Subject attribute definition		ESMPMPP	No	No	Yes	No
	ESM_EAU.2 Reliance on enterprise authentication		ESMPMPP	No	No	Yes	Yes
	ESM_EID.2 Reliance on enterprise identification		ESMPMPP	No	No	Yes	Yes
FAU - Security audit	FAU_GEN.1 Audit data generation		ESMPMPP	No	No	Yes	No
	FAU_SEL.1 Selective audit		ESMPMPP	No	No	Yes	Yes
	FAU_SEL_EXT.1 External selective audit		ESMPMPP	No	No	Yes	Yes
	FAU_STG_EXT.1 External audit trail storage		ESMPMPP	No	No	Yes	No
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation (for asymmetric keys)		ESMPMPP	No	No	No	Yes
	FCS_CKM_EXT.4 Cryptographic key zeroization		ESMPMPP	No	No	No	No

Security functional class	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)	FCS_COP.1	ESMPMPP	Yes	No	Yes	Yes
	FCS_COP.1(2) Cryptographic operation (for cryptographic signature)	FCS_COP.1	ESMPMPP	Yes	No	No	Yes
	FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)	FCS_COP.1	ESMPMPP	Yes	No	No	Yes
	FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)	FCS_COP.1	ESMPMPP	Yes	Yes	Yes	Yes
	FCS_HTTPS_EXT.1 HTTPS		ESMPMPP	No	No	No	No
	FCS_RBG_EXT.1 Cryptographic operation (random bit generation)		ESMPMPP	No	No	No	Yes
	FCS_SSH_EXT.1 SSH		ESMPMPP	No	No	Yes	Yes
	FCS_TLS_EXT.1(C) TLS client (syslog-ng)	FCS_TLS_EXT.1	ESMPMPP	Yes	No	No	Yes
	FCS_TLS_EXT.1(S) TLS server (HTTPS)	FCS_TLS_EXT.1	ESMPMPP	Yes	No	No	Yes
FIA - Identification and authentication	FIA_AFL.1 Authentication failure handling		ESMPMPP	No	No	Yes	Yes
	FIA_USB.1 User-subject binding		ESMPMPP	No	No	Yes	No
FMT - Security management	FMT_MOF.1 Management of security functions behavior		ESMPMPP	No	No	Yes	Yes
	FMT_MOF_EXT.1 External management of functions behavior		ESMPMPP	No	No	Yes	No
	FMT_MSA_EXT.5 Consistent security attributes		ESMPMPP	No	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		ESMPMPP	No	No	Yes	No
	FMT_SMR.1 Security roles		ESMPMPP	No	No	Yes	No
FPT - Protection of the TSF	FPT_APW_EXT.1 Protection of stored credentials		ESMPMPP	No	No	No	No
	FPT_SKP_EXT.1 Protection of secret key parameters		ESMPMPP	No	No	No	No

Security functional class	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FPT_STM.1 Reliable time stamps		ESMPMPP	No	No	No	No
FTA - TOE access	FTA_SSL.3 TSF-initiated termination		ESMPMPP	No	No	No	No
	FTA_SSL.4 User-initiated termination		ESMPMPP	No	No	No	No
	FTA_TAB.1 Default TOE access banners		ESMPMPP	No	No	No	No
	FTA_TSE.1 TOE session establishment		ESMPMPP	No	No	Yes	Yes
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		ESMPMPP	No	Yes	Yes	Yes
	FTP_TRP.1 Trusted path		ESMPMPP	No	No	No	Yes

6.1.1 (ESM)

6.1.1.1 ESM_ACD.1 Access control policy definition

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:

Subjects: **Defined in Table 6, Table 7, and Table 8**; and
 Objects: **Defined in Table 6, Table 7, and Table 8**; and
 Operations: **Defined in Table 6, Table 7, and Table 8**; and
 Attributes: **Defined in Table 6, Table 7, and Table 8**

Table 6: Computer Policy

Description	Subjects	Subject Attributes	Objects	Object Attributes	Operations
Session Inactivity Lock Screen	User	Username, Credentials	Session	Inactivity time limit	Automatically lock inactive session
Shutdown/ Restart Workstation From Lock Screen	User	None	Session Lock Screen Functions	Shutdown/ Restart Workstation Function	Shutdown/ Restart Workstation From Lock Screen

Description	Subjects	Subject Attributes	Objects	Object Attributes	Operations
Login With Allowed Authentication Methods	User	Username, Credentials	Authentication Function	Computer Policy » Authentication Methods	Login

Table 7: User Policy

Description	Subjects	Subject Attributes	Objects	Object Attributes	Operations
Failed Login Attempt Handling	User	Username, Credentials, User Policy » Consecutive Failed Login Attempts, User Policy » Failure Time Window, User Policy » Lockout time	Authentication Function		Login
Login With Allowed Authentication Methods	User	Username, Credentials, User Policy » Authentication Methods	Authentication Function		Login

Table 8: Combined Computer Policy and User Policy

Description	Subjects	Subject Attributes	Objects	Object Attributes	Operations
Login With Allowed Authentication Methods	User	Username, Credentials, User Policy » Authentication Methods	Authentication Function	Computer Policy » Authentication Methods	Login

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

TSS Link: [TSS for ESM_ACD.1](#)

6.1.1.2 ESM_ACT.1 Access control policy transmission

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: **at a periodic interval, when an agent authenticates a user, agent's first contact with the TOE.**

TSS Link: [TSS for ESM_ACT.1](#)

6.1.1.3 ESM_ATD.1 Object attribute definition

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: **Object attributes defined in Table 6, Table 7, and Table 8.**

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

TSS Link: [TSS for ESM_ATD.1](#)

6.1.1.4 ESM_ATD.2 Subject attribute definition

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: **Subject attributes defined in Table 6, Table 7, and Table 8.**

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

TSS Link: [TSS for ESM_ATD.2](#)

6.1.1.5 ESM_EAU.2 Reliance on enterprise authentication

ESM_EAU.2.1 The TSF shall rely on **the TOE's internal authentication server** 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.

TSS Link: [TSS for ESM_EAU.2](#)

6.1.1.6 ESM_EID.2 Reliance on enterprise identification

ESM_EID.2.1 The TSF shall rely on **the TOE's internal authentication server** for subject identification.

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.

TSS Link: [TSS for ESM_EID.2](#)

6.1.2 Security audit (FAU)

6.1.2.1 FAU_GEN.1 Audit data generation

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

- a) Start-up and shutdown of the audit functions; and
- b) All auditable events identified in [Table 9](#) for the not specified level of audit; and
- c) **no other auditable events.**

Table 9: Auditable events

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_EXT.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server <i>(including external audit log storage)</i>	Identification of audit server <i>(including external audit log storage)</i>
FCS_HTTPS_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_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(C), FCS_TLS_EXT.1(S)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the	Action taken when threshold is reached

Component	Event	Additional information
	actions taken when the threshold is reached, and any actions taken to restore the normal state	
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Modifications to the members of the management roles	None
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTA_TSE.1	Denial of session establishment	None
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_GEN.1.2** The TSF shall record within each audit record at least the following information:
- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
 - For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **no other audit relevant information beyond that defined in Table 9.**

TSS Link: *TSS for FAU_GEN.1*

6.1.2.2 FAU_SEL.1 Selective audit

- 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 from **local definition** based on the following attributes:
- event type;** and
 - no additional attributes.**

TSS Link: *TSS for FAU_SEL.1*

6.1.2.3 FAU_SEL_EXT.1 External selective audit

- FAU_SEL_EXT.1.1** The TSF shall be able to select the set of events to be audited by an ESM Access Control product from the set of all auditable events based on the following attributes:
- event type;** and
 - no additional attributes.**

TSS Link: [TSS for FAU_SEL_EXT.1](#)

6.1.2.4 FAU_STG_EXT.1 External audit trail storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to **both an external audit server and external audit log 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.

TSS Link: [TSS for FAU_STG_EXT.1](#)

6.1.3 Cryptographic support (FCS)

6.1.3.1 FCS_CKM.1 Cryptographic key generation (for asymmetric keys)

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys:¹

- **RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;**
- **ECC schemes using 'NIST curves' P-256, P-384 and P-521 that meet the following: FIPS 186-4, "Digital Signature Standard (DSS)", Appendix B.4**
- **FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526,**

used for key establishment in accordance with:

- **RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2;"**
- **Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A, Revision 3 "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography;"**
- **Finite field-based key establishment scheme using Diffie-Hellman Group 14 that meets the following: RFC 3526, Section 3;**

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

TSS Link: [TSS for FCS_CKM.1](#)

¹ [CCEVS-TD0573] was applied to [FCS_CKM.1](#).

6.1.3.2 FCS_CKM_EXT.4 Cryptographic key zeroization

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

TSS Link: [TSS for FCS_CKM_EXT.4](#)

6.1.3.3 FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in **CTR, CBC, GCM** mode and cryptographic key sizes 128-bits, 256-bits, and **no other key sizes** that meets the following:²

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

TSS Link: [TSS for FCS_COP.1\(1\)](#)

6.1.3.4 FCS_COP.1(2) Cryptographic operation (for cryptographic signature)

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services in accordance with³

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

that meets the following:

- **RSA Digital Signature Algorithm - FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5 using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5;**

TSS Link: [TSS for FCS_COP.1\(2\)](#)

6.1.3.5 FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm **SHA-1, SHA-256, SHA-384, SHA-512** and message digest sizes **160, 256, 384, 512** bits that meet the following: FIPS Pub 180-4, "Secure Hash Standard."⁴

TSS Link: [TSS for FCS_COP.1\(3\)](#)

6.1.3.6 FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)

FCS_COP.1.1(4) The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-**SHA-1, SHA-256, SHA-384, SHA-512**, key size **256 bits**, and message digest sizes **160, 256, 384, 512** bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code," and FIPS Pub 180-4, "Secure Hash Standard."⁵

TSS Link: [TSS for FCS_COP.1\(4\)](#)

² [CCEVS-TD0573] was applied to FCS_COP.1(1).

³ [CCEVS-TD0573] was applied to FCS_COP.1(2).

⁴ [CCEVS-TD0573] was applied to FCS_COP.1(3).

⁵ [CCEVS-TD0573] was applied to FCS_COP.1(4).

6.1.3.7 FCS_HTTPS_EXT.1 HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

TSS Link: [TSS for FCS_HTTPS_EXT.1](#)

6.1.3.8 FCS_RBG_EXT.1 Cryptographic operation (random bit generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with NIST Special Publication 800-90 using **Hash_DRBG (any), CTR_DRBG (AES)** seeded by an entropy source that accumulates entropy from **(2) one or more independent software-based noise sources**.⁶

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.

TSS Link: [TSS for FCS_RBG_EXT.1](#)

6.1.3.9 FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and **4256, 4344, 6668** as a **client**.⁷

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, and **password-based**.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than **32K** 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 and rejects all other encryption algorithms: aes128-ctr, aes256-ctr, **aes128-cbc, aes256-cbc**.

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses **ssh-rsa** and **no other public key algorithms** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512** and **no other MAC algorithms** as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSH_EXT.1.7 The TSF shall ensure that **diffie-hellman-group14-sha1** and **no other methods** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSH_EXT.1.8 The TSF shall ensure that the SSH connection be rekeyed after **no more than 1 Gigabyte of data has been transmitted** using that key.

Application Note: *This SFR is for SSH implemented by the appliance's Apache SSHD program (Bouncy Castle).*

TSS Link: [TSS for FCS_SSH_EXT.1](#)

⁶ [CCEVS-TD0079] was applied to FCS_RBG_EXT.1.

⁷ [CCEVS-TD0574] was applied to FCS_SSH_EXT.1.

6.1.3.10 FCS_TLS_EXT.1(C) TLS client (syslog-ng)

FCS_TLS_EXT.1.1(C) The product shall implement TLS 1.2 (RFC 5246) and **no earlier TLS versions** that supports the cipher suites⁸

- **TLS_RSA_WITH_AES_128_CBC_SHA** as defined in RFC 5246
- **TLS_RSA_WITH_AES_256_CBC_SHA** as defined in RFC 5246
- **TLS_RSA_WITH_AES_128_CBC_SHA256** as defined in RFC 5246
- **TLS_RSA_WITH_AES_256_CBC_SHA256** as defined in RFC 5246
- **TLS_RSA_WITH_AES_128_GCM_SHA256** as defined in RFC 5288
- **TLS_RSA_WITH_AES_256_GCM_SHA384** as defined in RFC 5288

Application Note: *This SFR is for TLS implemented by the appliance's syslog-ng client (OpenSSL).*

TSS Link: [TSS for FCS_TLS_EXT.1\(C\)](#)

6.1.3.11 FCS_TLS_EXT.1(S) TLS server (HTTPS)

FCS_TLS_EXT.1.1(S) The product shall implement TLS 1.2 (RFC 5246) and **no earlier TLS versions** that supports the cipher suites⁹

- **TLS_RSA_WITH_AES_128_CBC_SHA** as defined in RFC 5246
- **TLS_RSA_WITH_AES_256_CBC_SHA** as defined in RFC 5246
- **TLS_RSA_WITH_AES_128_CBC_SHA256** as defined in RFC 5246
- **TLS_RSA_WITH_AES_256_CBC_SHA256** as defined in RFC 5246
- **TLS_RSA_WITH_AES_128_GCM_SHA256** as defined in RFC 5288
- **TLS_RSA_WITH_AES_256_GCM_SHA384** as defined in RFC 5288
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256** as defined in RFC 5289
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** as defined in RFC 5289
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384** as defined in RFC 5289
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** as defined in RFC 5289

Application Note: *This SFR is for TLS implemented by the appliance's Apache HTTP Server (Apache NSS).*

TSS Link: [TSS for FCS_TLS_EXT.1\(S\)](#)

6.1.4 Identification and authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 1 to 99** unsuccessful authentication attempts occur related to **consecutive unsuccessful authentication events per account**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **prevent the user from logging in for a period of 5 minutes**.

TSS Link: [TSS for FIA_AFL.1](#)

⁸ [CCEVS-TD0621] was applied to FCS_TLS_EXT.1(C).

⁹ [CCEVS-TD0621] was applied to FCS_TLS_EXT.1(S).

6.1.4.2 FIA_USB.1 User-subject binding

- FIA_USB.1.1** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **roles**.
- 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:
- **Admin Console: Combine the administrator role attributes associated with all roles assigned to a user**
 - **Appliance Console: The Super Administrator user is associated with the Super Administrator role and the Administrator user is associated with the Administrator role.**
- 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:
- **Admin Console: Changes to roles and to user role assignments take effect on the next user login.**
 - **Appliance Console: Roles cannot be changed.**

TSS Link: [TSS for FIA_USB.1](#)

6.1.5 Security management (FMT)

6.1.5.1 FMT_MOF.1 Management of security functions behavior

- FMT_MOF.1.1** The TSF shall restrict the ability to **determine the behaviour of, disable, enable, modify the behaviour of** the functions: **listed in Table 10** to
- **Admin Console: The Super Administrator role and to the Delegated Administrator role with the administrator role attributes specified in Table 10**
 - **Appliance Console: The Super Administrator role and Administrator role specified in Table 10**

TSS Link: [TSS for FMT_MOF.1](#)

6.1.5.2 FMT_MOF_EXT.1 External management of functions behavior

- 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, **Refresh Interval** to **Admin Console Super Administrators and Delegated Administrators with the appropriate administrator role attributes**.

TSS Link: [TSS for FMT_MOF_EXT.1](#)

6.1.5.3 FMT_MSA_EXT.5 Consistent security attributes

- FMT_MSA_EXT.5.1** The TSF shall **only permit definition of unambiguous policies**.
- FMT_MSA_EXT.5.2** The TSF shall take the following action when an inconsistency is detected: **no action required**.

TSS Link: [TSS for FMT_MSA_EXT.5](#)

6.1.5.4 FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
the list of management functions in Table 10.

Table 10: Management functions

SFR	Management functions	Admin role attributes
ESM_ACD.1	Creation of policies	Admin Console: Create/Edit Computer Policy, Create/Edit User Policy
ESM_ACT.1	Transmission of policies	Admin Console: Update System Properties
ESM_ATD.1	Definition of object attributes. Association of attributes with objects.	Admin Console: Assign Computer Policy, Create/Edit Computer Policy
ESM_ATD.2	Definition of subject attributes. Association of attributes with subjects.	Admin Console: Add/Edit Users, Assign User Policy, Create/Edit User Policy
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Admin Console: Add/Edit Users, Delete Users
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Admin Console: Add/Edit Users, Delete Users
FAU_SEL.1	Configuration of auditable events	Admin Console: Update System Properties
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	Admin Console: Update System Properties
FAU_STG_EXT.1	Configuration of external audit storage location	Admin Console: Maintain Audit Log

SFR	Management functions	Admin role attributes
FIA_AFL.1	Configuration of authentication failure threshold value. Configuration of actions to take when threshold is reached. Execution of restoration to normal state following threshold action (if applicable).	Appliance Console: Super Administrator or Administrator
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	Admin Console: Add/Edit Users
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products	Admin Console: Assign Computer Policy, Assign User Policy, Create/Edit Computer Policy, Create/Edit User Policy, Maintain Audit Log, Update Computer Policy, Update System Properties
FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)	(Not applicable)
FMT_SMR.1	Management of the users that belong to a particular role	Admin Console: Create/Edit Administrator Roles, Delete Administrator Roles, Add/Edit Users
FTA_TAB.1	Maintenance of the banner	Admin Console: Update System Properties
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	Admin Console: Maintain Audit Log and/or Update System Properties Appliance Console: Super Administrator or Administrator
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	Appliance Console: Super Administrator or Administrator

Application Note: *The Super Administrator can perform all management functions. Delegated Administrators must have the specified administrator role attributes to perform the management function.*

TSS Link: [TSS for FMT_SMF.1](#)

6.1.5.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Admin Console: Super Administrator, Delegated Administrator**
- **Appliance Console: Super Administrator, Administrator**

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

TSS Link: [TSS for FMT_SMR.1](#)

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_APW_EXT.1 Protection of stored credentials

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.

TSS Link: [TSS for FPT_APW_EXT.1](#)

6.1.6.2 FPT_SKP_EXT.1 Protection of secret key parameters

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

TSS Link: [TSS for FPT_SKP_EXT.1](#)

6.1.6.3 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

TSS Link: [TSS for FPT_STM.1](#)

6.1.7 TOE access (FTA)

6.1.7.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after an Authorized Administrator-configurable time interval of session inactivity.

TSS Link: [TSS for FTA_SSL.3](#)

6.1.7.2 FTA_SSL.4 User-initiated termination

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

TSS Link: [TSS for FTA_SSL.4](#)

6.1.7.3 FTA_TAB.1 Default TOE access banners

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

TSS Link: [TSS for FTA_TAB.1](#)

6.1.7.4 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **the interface and attributes defined in Table 11.**

Table 11: TOE session establishment

Interface	Attributes
Admin Console	Day, time, duration, and user role
Appliance Console	Username

TSS Link: [TSS for FTA_TSE.1](#)

6.1.8 Trusted path/channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be capable of using **SSH, TLS, HTTPS** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **external audit server (TLS), external audit log storage (SSH), agent (HTTPS)** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.¹⁰

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities 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, **audit data transfer.**

TSS Link: [TSS for FTP_ITC.1](#)

6.1.8.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall be capable of using **HTTPS** to provide a trusted communication path between itself and remote users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification, disclosure, and **no other types of integrity or confidentiality violations.**¹¹

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

¹⁰ [CCEVS-TD0576] was applied to FTP_ITC.1.

¹¹ [CCEVS-TD0576] was applied to FTP_TRP.1.

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

TSS Link: [TSS for FTP_TRP.1](#)

6.2 Security Functional Requirements Rationale

Any security functional requirements rationale is provided by the PPs to which this ST conforms.

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are defined in [CC] part 3 for the Evaluation Assurance Level 1.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.), and selection (Sel.).

Table 12: SARs

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_FSP.1 Basic functional specification	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.1 Labelling of the TOE	CC Part 3	No	No	No	No
	ALC_CMS.1 TOE CM coverage	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_OBJ.1 Security objectives for the operational environment	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.1 Stated security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_IND.1 Independent testing - conformance	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.1 Vulnerability survey	CC Part 3	No	No	No	No

6.4 Security Assurance Requirements Rationale

Security assurance requirements rationale is provided by the PPs to which this ST conforms.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 ESM_ACD.1 Access control policy definition

SFR Link: ESM_ACD.1

The Access Control products are the Imprivata Agents (a.k.a. agents) each running on a separate Windows 10 OS endpoint. The agents are specifically designed to work with the Imprivata Appliance.

Computer Policy

In the evaluated configuration, the Computer Policy determines the authentication methods available to a user on that endpoint and controls access to certain endpoint features. A Computer Policy is assigned and transferred to each registered endpoint and is enforced by the agent on that endpoint. Below is a description of each tested feature. [Table 6](#) and [Table 8](#) provide the subject, object, operations, and attributes which are also described below.

Each Computer Policy has a unique Computer Policy ID and unique name to identify the policy. Each Computer Policy can be assigned to one or more endpoints. The TOE maintains the mapping of endpoints to Computer Policies.

Session Inactivity Lock Screen

This maps to the "Walk-Away Security » Inactivity detection » Keyboard and mouse" portion of the Computer Policy. This function requires an established user session (i.e., a user to be logged in to the endpoint). The user must have a valid username and credentials defined to the TOE in order to establish a session. The session tracks the last time a user used the keyboard or moved the mouse. The Computer Policy supplies an inactivity time limit (a.k.a. timeout period) for all user sessions. If the session is inactive for the specified inactivity time limit, then the session initiates a lock screen.

Shutdown/Restart Workstation From Lock Screen

This maps to the "General » Shutdown/restart workstation from lock screen" portion of the Computer Policy. This function requires an established user session (i.e., a user to be logged in to the endpoint) and the lock screen to be active. The lock screen can display or not display a shutdown/restart button. This button allows an unknown user to shutdown or restart the endpoint from the lock screen without first authenticating, thus effectively terminating the locked session. The Computer Policy allows the administrator to enable (display) or disable (hide) this Shutdown/Restart Workstation lock screen function (button). Because the user who clicks the displayed button is unknown, there are no subject attributes associated with this operation.

Login With Allowed Authentication Methods

This maps to the "Override and Restrict » Desktop Access Authentication Restrictions » Restrict user policy" portion of the Computer Policy. The Computer Policy can restrict the set of authentication methods available to any authenticating user. The user must have a valid username and credentials defined to the TOE in order to log in. The user must also authenticate using an authentication method allowed by the Computer Policy.

User Policy

In the evaluated configuration, the User Policy determines the authentication methods available to the user and controls certain endpoint features. A User Policy is assigned to each user account and is enforced by the agent on that endpoint. Below is a description of each tested feature. [Table 7](#) and [Table 8](#) provide the subject, object, operations, and attributes which are also described below.

Each User Policy has a unique User Policy ID and unique name to identify the policy. Each User Policy can be assigned to one or more user accounts. The TOE maintains the mapping of usernames to User Policy IDs.

Failed Login Attempt Handling

This maps to the "Authentication » Lockout" portion of the User Policy. This function tracks a User Policy-configurable number of consecutive failed login attempts of a user in a User Policy-configurable time window (failure time window). If the number is reached within the time window, then the agent prevents the user from logging in until a User Policy-configurable amount of time has passed (lockout time). The user must have a valid username and credentials defined to the TOE. No object attributes are required for this.

Login With Allowed Authentication Methods

This maps to the "Authentication » Primary factors" portion of the User Policy. The User Policy can restrict the set of authentication methods available to the user. The user must have a valid username and credentials defined to the TOE in order to log in. The user must also authenticate using an authentication method allowed by the User Policy.

Combined Computer Policy and User Policy

In the evaluated configuration, for a user to authenticate to an endpoint, both the user and the endpoint must be enrolled with the TOE. Enrollment enforces that the user has an assigned User Policy and the endpoint has an assigned Computer Policy. The user must also have a valid username and credentials. The agent combines the Computer Policy and User Policy to determine the user's set of authentication methods. [Table 8](#) provides the subject, object, operations, and attributes which are also described below.

Login With Allowed Authentication Methods

This maps to the "Override and Restrict » Desktop Access Authentication Restrictions » Restrict user policy" portion of the Computer Policy and the "Authentication » Primary factors" portion of the User Policy. The Computer Policy can restrict the set of authentication methods available to any authenticating user. The User Policy can restrict the set of authentication methods available to the authenticating user. The intersection of the two restrictive policies determines the authentication methods available to the authenticating user. It is possible for that intersection to be an empty set, in which case, the user will not be able to log in to the endpoint.

7.1.2 ESM_ACT.1 Access control policy transmission

SFR Link: [ESM_ACT.1](#)

The Access Control products are the Imprivata Agents (a.k.a. agents) each running on a separate Windows 10 OS endpoint. The agents are specifically designed to work with the Imprivata Appliance.

Computer Policy

The TOE transmits the Computer Policy to the agent at every Refresh Interval and each time a user initiates a log in on an endpoint. The agent sends its unique ID to the TOE. The TOE responds with the agent's matching Computer Policy. Similarly, when the agent contacts the TOE for the first time, the TOE responds by sending a default Computer Policy. This connection is protected as specified in [FTP_ITC.1](#).

User Policy

The TOE transmits the User Policy to the agent each time a user initiates a log in on an endpoint (and also at every Refresh Interval while the user is logged in). The agent sends the username to the TOE. The TOE responds with the matching User Policy. Agents are configured to deny a login if they are unable to connect to the TOE and obtain the User Policy. This connection is protected as specified in [FTP_ITC.1](#).

7.1.3 ESM_ATD.1 Object attribute definition

SFR Link: [ESM_ATD.1](#)

The object attributes and their purposes are described in the [TSS for ESM_ACD.1 section 7.1.1](#).

7.1.4 ESM_ATD.2 Subject attribute definition

SFR Link: [ESM_ATD.2](#)

The subject attributes and their purposes are described in the [TSS for ESM_ACD.1 section 7.1.1](#).

7.1.5 ESM_EAU.2 Reliance on enterprise authentication

SFR Link: [ESM_EAU.2](#)

Enterprise users (i.e., users on the endpoints) and Admin Console users authenticate through the same enterprise authentication mechanism—the TOE's internal authentication server which uses the TOE's database to store user accounts. In all cases, the user/subject must be identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note: The Appliance Console does not use enterprise authentication and identification; therefore, it is not included in either [ESM_EAU.2](#) or [ESM_EID.2](#). The Appliance Console is a low-use administrative interface, used only for low-level configuration. Its users authenticate via a local password file on the TOE. Only two accounts exist in this password file: Super Administrator and Administrator. Neither are enterprise accounts. In all cases, the user/subject must be identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.6 ESM_EID.2 Reliance on enterprise identification

SFR Link: [ESM_EID.2](#)

The information for this TSS has been included in the [TSS for ESM_EAU.2 section 7.1.5](#).

7.1.7 FAU_GEN.1 Audit data generation

SFR Link: [FAU_GEN.1](#)

The TOE generates audit records for the events specified in [Table 9](#). The audit records contain the additional information specified in the table. In addition, the TOE generates audit records for the audit trail startup and shutdown events.

Each audit record contains the following information:

- Date and time of the event
- Type of event
- Subject identity (if applicable)
- Outcome
- Additional information specified in [Table 9](#)

7.1.8 FAU_SEL.1 Selective audit

SFR Link: [FAU_SEL.1](#)

An Admin Console administrator with the *Update System Properties* administrator role attribute can select the "event type" of the audit events audited by the TOE via the Admin Console under System Settings.

7.1.9 FAU_SEL_EXT.1 External selective audit

SFR Link: [FAU_SEL_EXT.1](#)

An administrator on the TOE can configure/select the "event type" of the audit events audited by the agents via the Admin Console under System Settings. See the FAU_SEL_EXT.1 entry in [Table 21](#) of the TSS for FMT_SMF.1 section 7.1.27 for additional information.

7.1.10 FAU_STG_EXT.1 External audit trail storage

SFR Link: [FAU_STG_EXT.1](#)

The TOE uses two separate local auditing mechanisms to fulfill the audit requirements. Different events are recorded by each mechanism. One mechanism stores audit records in the TOE's local database. The other mechanism uses syslog and a local syslog file. In both cases, the audit records are protected from unauthorized deletion and modification. The TOE only allows administrators with the appropriate administrator role attributes access to the audit records.

The audit records in the TOE's local database can be saved to external audit log storage using SSH to protect the channel. The syslog audit records can be saved to an external audit server (syslog server) using TLS to protect the channel. The TSS for FTP_ITC.1 section 7.1.36 provides additional trusted channel details.

Table 13: Audit storage mechanisms

Mechanism #	Local	External	Secure channel
1	Local database	External audit log storage	SSH
2	Local syslog file	External audit server (syslog)	TLS

External audit log storage

The external audit log storage mechanism can be configured to transfer audit records two different ways: periodically or on-demand. When configured for periodic transfers, the TOE automatically transfers audit records in log files to the external audit log storage at administrator-defined intervals. If the connection fails during the transfer or the external audit log storage is unavailable, the TOE retains the log files and attempts to transfer them at the next interval. When configured for on-demand transfers, the TOE transfers audit records in log files to the external audit log storage at the request of the administrator. If the connection fails during the transfer or the external audit log storage is unavailable, the TOE retains the log files and the administrator must reattempt the transfer. In both cases, audit record data is not lost.

External audit server (syslog)







The external audit server mechanism connects and continuously sends audit records to the external audit server. If the connection fails or the external audit server is unavailable, all audit events generated while the connection is broken are lost. When the connection is re-established, only audit records generated after the re-establishment are sent to the external audit server. No alert or notification is provided to the administrator regarding these lost audit records.

7.1.11 FCS_CKM.1 Cryptographic key generation (for asymmetric keys)

SFR Link: [FCS_CKM.1](#)

Table 14 lists the cryptographic modules and, for each module, the asymmetric algorithms, key sizes, curves, standards, and usages used to satisfy the ST claims. (SP800-56B Key Establishment is not claimed.)

Table 14: Asymmetric key generation, verification, and establishment algorithms

Module	Algorithm	Capabilities	Standard	CAVP #	Usage
Apache NSS	ECDSA KeyGen/KeyVer	Curves: P-256, P-384, P-521	[FIPS186-4] 	A3233	HTTPS server
	RSA key establishment	Modulo: 2048	[RFC8017] 	None	
	Elliptic curve-based key establishment (KAS-ECC-SSC Sp800-56Ar3)	Curves: P-256, P-384, P-521	[SP800-56A-Rev3] 	A3233	
Bouncy Castle	RSA KeyGen	Modulo: 2048	[FIPS186-4] 	A3227	SSH client authentication key pair generation
	Finite field-based key establishment	Diffie-Hellman Group 14	[RFC3526] 	None	SSH client
OpenSSL	RSA key establishment	Modulo: 2048, 3072, 4096	[RFC8017] 	None	TLS client

Note: Cryptographic algorithms marked as "None" in the "CAVP #" column are not tested through the CAVP. Instead, requirements in the corresponding testing assurance activities have been followed.

7.1.12 FCS_CKM_EXT.4 Cryptographic key zeroization

SFR Link: [FCS_CKM_EXT.4](#)

Table 15 lists the secret keys, private keys, and critical security parameters, the storage location type, when the values are destroyed, and the destruction method.

Table 15: Key destruction

Application	Secret type	Storage location	When destroyed	Destruction method
Apache SSHD (SSH client - Bouncy Castle)	AES session keys (both)	Volatile	After session completion	Single overwrite with zeros
	DRBG seed material	Volatile	After use	Single overwrite with zeros
	DH keys	Volatile	After session establishment	Single overwrite with zeros
	RSA private key (public key auth)	Volatile	After session establishment	Single overwrite with zeros
	Client password (password-based auth)	Volatile	After session establishment	Single overwrite with zeros
Apache HTTPS Server (TLS - Apache NSS)	AES session key	Volatile	After session completion	Single overwrite with zeros
	DRBG seed material	Volatile	After use	Single overwrite with zeros
	ECDHE keys	Volatile	After session establishment	Single overwrite with zeros
	ECDSA private keys	Volatile	After session establishment	Single overwrite with zeros
	Pre-master secret	Volatile	After session establishment	Single overwrite with zeros
	RSA private key	Volatile	After session establishment	Single overwrite with zeros
		Non-volatile	Never	
syslog-ng (TLS client - OpenSSL)	AES session key	Volatile	After session completion	Single overwrite with zeros
	DRBG seed material	Volatile	After use	Single overwrite with zeros
Apache HTTPS Server	Login passwords from Admin Console	Volatile	After session establishment	Single overwrite with zeros
	User login passwords from agents	Volatile	After session establishment	Single overwrite with zeros
	Unique 128-bit agent identifier/key	Volatile	After session termination	Single overwrite with zeros

Application	Secret type	Storage location	When destroyed	Destruction method
	Database symmetric encryption key	Volatile	Power off	Power loss
		Non-volatile	Never	

7.1.13 FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)

SFR Link: [FCS_COP.1\(1\)](#)

Table 16 lists the cryptographic modules and, for each module, the symmetric algorithms, modes, key sizes, and standards used to satisfy the ST claims.

Table 16: Symmetric encryption/decryption algorithms

Module	Algorithm	Capabilities	Standard	CAVP #	Usage
Apache NSS	AES-CBC	Direction: Encrypt, decrypt Key lengths: 128, 256 (bits)	[FIPS197], [SP800-38A]	A3233	HTTPS server
	AES-GCM	Direction: Encrypt, decrypt Key length: 128, 256 (bits) Tag length: 128 (bits) IV length: 96 (bits)	[FIPS197], [SP800-38D]		
Bouncy Castle	AES-CBC	Direction: Encrypt, decrypt Key lengths: 128, 256 (bits)	[FIPS197], [SP800-38A]	A3227	SSH client
	AES-CTR	Direction: Encrypt, decrypt Key lengths: 128, 256 (bits)	[FIPS197], [SP800-38A]		
OpenSSL	AES-CBC	Direction: Encrypt, decrypt Key lengths: 128, 256 (bits)	[FIPS197], [SP800-38A]	A899	TLS client
	AES-GCM	Direction: Encrypt, decrypt Key lengths: 128, 256 (bits) Tag length: 128 (bits) IV length: 96 (bits)	[FIPS197], [SP800-38D]		

7.1.14 FCS_COP.1(2) Cryptographic operation (for cryptographic signature)

SFR Link: [FCS_COP.1\(2\)](#)

Table 17 lists the cryptographic modules and, for each module, the signature algorithms, capabilities, and standards used to satisfy the ST claims.

Table 17: Signature generation/verification algorithms

Module	Algorithm	Capabilities	Standard	CAVP #	Usage
Apache NSS	RSA SigGen	Signature Type: PKCS 1.5 Moduli: 2048 with SHA-1	[FIPS186-4]	None	HTTPS server
		Signature Type: PKCS 1.5 Moduli: 2048 with SHA2-256, SHA2-384, SHA2-512	[FIPS186-4]	A3233	
Bouncy Castle	RSA SigGen	Signature Type: PKCS 1.5 Moduli: 2048 with SHA-1	[FIPS186-4]	None	SSH client
	RSA SigVer	Signature Type: PKCS 1.5 Moduli: 2048, 3072, 4096 with SHA-1	[FIPS186-4]	A3227	
OpenSSL	RSA SigVer	Signature Type: PKCS 1.5 Moduli: 2048, 3072, 4096 with SHA-1, SHA2-256, SHA2-384, SHA2-512	[FIPS186-4]	A899	TLS client

Note: Cryptographic algorithms marked as "None" in the "CAVP #" column are not tested through the CAVP. Instead, requirements in the corresponding testing assurance activities have been followed.

7.1.15 FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)

SFR Link: [FCS_COP.1\(3\)](#)

Table 18 lists the cryptographic modules and, for each module, the hash algorithms, capabilities, and standards used to satisfy the ST claims.

Table 18: Hash algorithms

Module	Algorithm	Capabilities	Standard	CAVP #	Usage
Apache NSS	SHA-1, SHA2-256, SHA2-384, SHA2-512	160 bits, 256 bits, 384 bits, 512 bits (Byte oriented)	[FIPS180-4]	A3233	HTTPS server: ECC key establishment, RSA SigGen & SigVer, HMACs, TLS PRFs, Hash_DRBG
Bouncy Castle	SHA-1, SHA2-256, SHA2-512	160 bits, 256 bits, 512 bits (Byte oriented)	[FIPS180-4]	A3227	SSH client: DH key establishment, RSA SigGen & SigVer, HMACs, Hash_DRBG
OpenSSL	SHA-1, SHA2-256, SHA2-384, SHA2-512	160 bits, 256 bits, 384 bits, 512 bits (Byte oriented)	[FIPS180-4]	A899	TLS client: RSA SigGen & SigVer, HMACs, TLS PRFs

7.1.16 FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)

SFR Link: [FCS_COP.1\(4\)](#)

Table 19 lists the cryptographic modules and, for each module, the keyed-hash algorithms, hash functions, key lengths, block sizes, and output MAC lengths used to satisfy the ST claims. All algorithms are byte oriented and meet [\[FIPS198-1\]](#) and [\[FIPS180-4\]](#).

Table 19: Keyed-hash message authentication algorithms

Module	Algorithm	Hash function	Key length (bits)	Block size (bits)	Output MAC length (bits)	CAVP #	Usage
Apache NSS	HMAC-SHA-1	SHA-1	256	512	160	A3233	HTTPS server
	HMAC-SHA2-256	SHA2-256	256	512	256		
	HMAC-SHA2-384	SHA2-384	256	1024	384		
Bouncy Castle	HMAC-SHA-1	SHA-1	256	512	160	A3227	SSH client
	HMAC-SHA2-256	SHA2-256	256	512	256		
	HMAC-SHA2-512	SHA2-512	256	1024	512		
OpenSSL	HMAC-SHA-1	SHA-1	256	512	160	A899	TLS client
	HMAC-SHA2-256	SHA2-256	256	512	256		
	HMAC-SHA2-384	SHA2-384	256	1024	384		

7.1.17 FCS_HTTPS_EXT.1 HTTPS

SFR Link: [FCS_HTTPS_EXT.1](#)

The TOE, specifically its Apache HTTP Server, acts as an HTTPS server handling inbound HTTPS requests. It provides the HTTPS connection compliant with [\[RFC2818\]](#) defaulting to port 443. Upon receiving an inbound request, it first establishes a TLS connection with the initiating endpoint, then it waits for the endpoint to initiate a request.

The TLS implementation for HTTPS is defined in [FCS_TLS_EXT.1\(S\)](#) and described in the TSS for [FCS_TLS_EXT.1\(S\)](#) section 7.1.21. It uses the Apache NSS cryptographic module. The following are the cryptographic functions used for HTTPS.

- Asymmetric key generation, verification, and establishment as per [FCS_CKM.1](#)
- Key destruction as per [FCS_CKM_EXT.4](#)
- Symmetric encryption/decryption as per [FCS_COP.1\(1\)](#)
- Signature generation and verification as per [FCS_COP.1\(2\)](#)
- Hash algorithms as per [FCS_COP.1\(3\)](#)
- Keyed-hash algorithms as per [FCS_COP.1\(4\)](#)
- DRBG for key and CSP generation as per [FCS_RBG_EXT.1](#)

The TOE receives inbound HTTPS requests from administrative web browsers and agents.

Web browsers

HTTPS is used by the TOE for the administrative browser interfaces: Admin Console and Appliance Console. A browser initiates the connection to the TOE; thus, the browser is expected to validate the X.509v3 certificate returned by the TOE via the TLS handshake protocol. The TOE provides assured identification by validating the browser's user via username/password after the TLS connection is established.

Agents

HTTPS is used by the TOE for communicating with the agents. An agent initiates the connection to the TOE; thus, the agent is expected to validate the X.509v3 certificate returned by the TOE during the TLS handshake protocol. Agents support the following two methods of assured identification.

- 1) When a user logs into a managed endpoint, the TOE provides assured identification by validating the agent's user via the user's username/password after the TLS connection is established.
- 2) When the agent contacts the TOE when no user is logged into the endpoint (i.e., during a Refresh Interval), the agent uses its unique key to identify itself to the TOE after the TLS connection is established. (For more information on the unique agent key, see [FTP_ITC.1](#).)




7.1.18 FCS_RBG_EXT.1 Cryptographic operation (random bit generation)

SFR Link: [FCS_RBG_EXT.1](#)

The TOE's cryptographic modules use the `/dev/random` device as their entropy source, which is a software-based noise source. Each DRBG is seeded from this source with a minimum of 256 bits of entropy. The `/dev/random` device blocks until its entropy estimator determines that sufficient entropy exists to fulfill the request.

[Table 20](#) lists the cryptographic modules and, for each module, the DRBG algorithm, capabilities, and standards used to satisfy the ST claims.

Table 20: DRBG algorithms

Module	Algorithm	Capabilities	Standard	CAVP #	Usage
Apache NSS	Hash_DRBG	Mode: SHA2-256	[SP800-90A-Rev1] 	A3233	HTTPS server
Bouncy Castle	Hash_DRBG	Mode: SHA2-256	[SP800-90A-Rev1] 	A3227	SSH client
OpenSSL	CTR_DRBG	Mode: AES-256	[SP800-90A-Rev1] 	A899	TLS client

7.1.19 FCS_SSH_EXT.1 SSH

SFR Link: [FCS_SSH_EXT.1](#)

Protocol: SSHv2 client
Application: Apache SSHD
Module: Bouncy Castle v1.68

The TOE, specifically Apache SSHD, implements the SSHv2 client protocol including SCP. SCP is used to protect the transfer of audit logs to external audit log storage. Apache SSHD requires Apache MINA, which requires Java VM. Java VM uses the Bouncy Castle v1.68 software library (a.k.a. module) as its cryptographic provider.

Apache SSHD is compliant with RFCs 4251, 4252, 4253, and 4254 supporting port forwarding as specified in [RFC4254] section 7 for clients and a maximum packet length of 32K bytes as specified in [RFC4253] section 6.1. If a packet is larger than 32K bytes, the packet is dropped (i.e., discarded). It is also compliant with the following.

- [RFC4256] supporting generic message exchange authentication
- [RFC4344] supporting the aes128-ctr, aes256-ctr, and other algorithms
- [RFC6668] supporting HMACs with SHA-2

Apache SSHD supports both public key-based and password-based authentication methods as per [RFC4252]. The TOE supports the following PP-specified transport public key authentication algorithm and rejects all others. (See the TSS for FCS_COP.1(2) section 7.1.14.)

- ssh-rsa (i.e., RSA signatures with PKCS1 1.5 and SHA-1)

The TOE supports the following PP-specified encryption algorithms and rejects all others. (See the TSS for FCS_COP.1(1) section 7.1.13.)

- aes128-cbc
- aes256-cbc
- aes128-ctr
- aes256-ctr

The TOE supports the following PP-specified data integrity algorithms and rejects all others. (See the TSS for FCS_COP.1(4) section 7.1.16.)

- hmac-sha1
- hmac-sha1-96¹²
- hmac-sha2-256
- hmac-sha2-512

The TOE supports the following key exchange/establishment method and rejects all others. (See the TSS for FCS_CKM.1 section 7.1.11.)

- diffie-hellman-group14-sha1

The TOE will automatically rekey a connection after the following conditions:

- no more than 1 Gigabyte of data has been transmitted

RSA 2048-bit keys used for SSH client key-based authentication are generated using the Bouncy Castle cryptographic module. (See the TSS for FCS_CKM.1 section 7.1.11.)

The TOE uses the PP-specified DRBG shown in the TSS for FCS_RBG_EXT.1 section 7.1.18.

7.1.20 FCS_TLS_EXT.1(C) TLS client (syslog-ng)

SFR Link: FCS_TLS_EXT.1(C)

Protocol: TLS 1.2 (client)

¹² hmac-sha1-96 is a truncated version of HMAC-SHA-1.

Application: syslog-ng client
Module: OpenSSL v1.0.2p

The TOE, specifically its syslog-ng client, acts as a TLS client when communicating with the external audit server (syslog server).

The syslog-ng client supports TLS 1.2 ([RFC5246][1](#)) for communicating with the external audit server (syslog). It rejects all other TLS versions of the protocol and all SSL versions. It uses the OpenSSL v1.0.2p software library (a.k.a. module) for its TLS implementation and cryptographic provider.

The syslog-ng client supports the following PP-specified TLS ciphersuites.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

7.1.21 FCS_TLS_EXT.1(S) HTTPS server

SFR Link: [FCS_TLS_EXT.1\(S\)](#)

Protocol: TLS 1.2 (server)
Application: Apache HTTP Server
Module: Apache NSS v3.77

The TOE, specifically its Apache HTTP Server, acts as an HTTPS server handling inbound HTTPS requests.

The Apache HTTP Server supports TLS 1.2 ([RFC5246][1](#)) for HTTPS connections. It rejects all other TLS versions of the protocol and all SSL versions. It uses the Apache NSS v3.77 software library (a.k.a. module) for its TLS implementation and cryptographic provider.

The Apache HTTP Server supports the following PP-specified TLS ciphersuites with HTTPS.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

7.1.22 FIA_AFL.1 Authentication failure handling

SFR Link: [FIA_AFL.1](#)

For the Admin Console and Appliance Console, the TOE detects consecutive unsuccessful authentication attempts per account and then locks the account for 5 minutes. The number of consecutive unsuccessful authentication attempts is administrator-configurable from 1 to 99.

7.1.23 FIA_USB.1 User-subject binding

SFR Link: [FIA_USB.1](#)

For the Admin Console, each administrator has one or more roles (security attribute) assigned to their account in the TOE's database. When an administrator successfully logs in to the TOE, the administrator role attributes of each role assigned to the administrator are combined to provide the administrator their full access rights. Changes to either the administrator role attributes assigned to a role or to the roles assigned to an administrator during the administrator's active session do not take effect until the next time the user logs back in to the TOE. Roles can be assigned to administrators as specified in the FMT_SMR.1 entry of [Table 21](#) in the [TSS for FMT_SMF.1 section 7.1.27](#).

For the Appliance Console, there are two accounts and two roles. The Super Administrator account is bound to the Super Administrator role. The Administrator account is bound to the Administrator role.

7.1.24 FMT_MOF.1 Management of security functions behavior

SFR Link: [FMT_MOF.1](#)

The information for this TSS has been included in the [TSS for FMT_SMF.1 section 7.1.27](#).

7.1.25 FMT_MOF_EXT.1 External management of functions behavior

SFR Link: [FMT_MOF_EXT.1](#)

The TOE supports the following required agent management functions. Keep in mind that, in the OneSign architecture, the TOE never contacts the agent. Instead, the agents contact the TOE under the conditions described in [section 1.5.2.1.5](#).

Audited events

An administrator on the TOE can both **query** and **modify** the set of rules for excluding audited events from a master set of events of all agents via the Admin Console. The administrator must have the *Update System Properties* administrator role attribute for these operations. (Related SFR: [FAU_SEL_EXT.1](#))

The agent's audit events are sent to the TOE for storage. Using the Admin Console, an administrator can view an agent's audit records stored on the TOE and determine that the set of audit events are being audited by the agent.

Repository for trusted audit storage

An administrator on the TOE can **query** and **modify** the agent's repository location for the audit log storage via the Admin Console. The administrator must have the *Maintain Audit Log* administrator role attribute for these operations.

Because the TOE never contacts the agent, the agent sends the current location of the repository to the TOE on every Refresh Interval. The Admin Console displays the repository location last received from the agent at its Refresh Interval.

Access control SFP

Computer Policy

An administrator on the TOE can **query** and **modify** the Computer Policy currently enforced by the agent via the Admin Console. The administrator must have the *Create/Edit Computer Policy* administrator role attribute for these operations.

User Policy

An administrator on the TOE can **query** and **modify** the User Policy currently enforced by the agent via the Admin Console. The administrator must have the *Create/Edit User Policy* administrator role attribute for these operations.

Because the TOE never contacts the agent, the agent sends the current User Policy ID and Computer Policy ID to the TOE on every Refresh Interval. The Admin Console displays the User Policy ID and Computer Policy ID last received from the agent at its Refresh Interval.

Policy being implemented by the TSF¹³

An administrator on the TOE can **query** the User Policy and Computer Policy currently enforced by the agent and apply (**modify**) a different User Policy and Computer Policy to be enforced by the agent via the Admin Console. The administrator must have the *Assign User Policy* and *Assign Computer Policy* administrator role attributes for these operations.

Because the TOE never contacts the agent, the agent sends the current User Policy ID and Computer Policy ID to the TOE on every Refresh Interval. The Admin Console displays the User Policy ID and Computer Policy ID last received from the agent at its Refresh Interval.

Access control SFP behavior to enforce in the event of communications outage

In the evaluated configuration, the agent is required to have Offline Authentication mode disabled. When Offline Authentication mode is disabled, if there is an agent communication outage with the TOE, then the agent terminates any active user sessions and disallows any new logins until a connection to the TOE can be re-established. In addition, when Offline Authentication mode is disabled, local Windows 10 OS authentication is disabled preventing users from bypassing the OneSign authentication mechanism. Therefore, by configuration, the access control SFP behavior is to disallow all access to objects until the connection between the agent and the TOE is re-established.

An administrator on the TOE can **query** and **modify** the agent's Offline Authentication mode via the Admin Console. The administrator must have the *Create/Edit User Policy* administrator role attribute for these operations.

Refresh Interval

The Refresh Interval is a global value that applies to all agents and is sent to each agent when the TOE sends a Computer Policy to an agent.

An administrator on the TOE can **query** and **modify** the global Refresh Interval value under the Settings menu of the Admin Console. The administrator must have the *Update System Properties* administrator role attribute for these operations. When the Refresh Interval is modified, the new Refresh Interval is applied to the endpoint the next time the endpoint's agent contacts the TOE. The agents contact the TOE under the conditions described in [section 1.5.2.1.5](#).

¹³ Although FMT_MOF_EXT.1 uses the wording "policy version being implemented", its assurance activity uses the wording "policy being implemented by the TSF."

7.1.26 FMT_MSA_EXT.5 Consistent security attributes

SFR Link: [FMT_MSA_EXT.5](#)

The Computer Policy has no internal inconsistencies within the policy. The User Policy has no internal inconsistencies within the policy. Each controlled item is independent of the others. Controlled items can be enabled or disabled. Default values exist for attributes and sub-attributes of a controlled item, so there is never a lack of an in-range value.

It is possible for the Computer Policy and User Policy to have differing sets of authentication methods between them when combined at the agent. See [TSS for ESM_ACD.1 section 7.1.1](#) for a discussion on this topic. But, the combining of policies is out of the scope of this requirement.

7.1.27 FMT_SMF.1 Specification of management functions

SFR Link: [FMT_SMF.1](#)

[Table 21](#) provides a summary of the available management functions. On the Admin Console, the Super Administrator role can perform all management functions. The Delegated Administrator role must have the administrator role attributes specified in [Table 21](#).

Table 21: Security management functions

SFR	Management functions	Admin role attributes
ESM_ACD.1	Creation of policies	Admin Console: Create/Edit Computer Policy, Create/Edit User Policy
	<p>Summary</p> <p>An administrator can create Computer Policies and User Policies (a.k.a. access control policies).</p>	
ESM_ACT.1	Transmission of policies	Admin Console: Update System Properties
	<p>Summary</p> <p>An agent contacts the TOE at a Refresh Interval to receive updated policies. An administrator can set the agent Refresh Interval via the Admin Console.</p>	
ESM_ATD.1	Definition of object attributes. Association of attributes with objects.	Admin Console: Assign Computer Policy, Create/Edit Computer Policy
	<p>Summary</p> <p>Object attributes from ESM_ACD.1:</p> <ul style="list-style-type: none"> • Computer Policy » Inactivity time limit—Session attribute specifying the maximum amount of inactivity time before the session locks the user's screen. • Computer Policy » Shutdown/Restart Workstation Function—Lock screen attribute specifying if the "Shutdown/Restart Workstation Function" is enabled or disabled. • Computer Policy » Authentication Methods—Login attribute specifying the list of Computer Policy-allowed endpoint authentication methods. 	

SFR	Management functions	Admin role attributes
	<p>Using the Admin Console, the administrator can assign a Computer Policy to an endpoint as well as modify the Computer Policy-related object attributes listed above within a Computer Policy.</p> <p>When the endpoint receives the Computer Policy, the endpoint's agent associates the Computer Policy-related object attributes with the object.</p>	
ESM_ATD.2	<p>Definition of subject attributes.</p> <p>Association of attributes with subjects.</p>	<p>Admin Console: Add/Edit Users, Assign User Policy, Create/Edit User Policy</p>
	<p>Summary</p> <p>Subject attributes from ESM_ACD.1:</p> <ul style="list-style-type: none"> • Username—User attribute specifying the user's username defined in the authentication server. • Credentials—User attribute specifying the user's credentials defined in the authentication server. • User Policy » Consecutive Failed Login Attempts—User attribute specifying the maximum number of consecutive failed logins (within a time window) before an account lockout is initiated. • User Policy » Failure Time Windows—User attribute specifying the time window for the consecutive failed logins to occur. • User Policy » Lockout Time—User attribute specifying the amount of time the user account will remain locked. • User Policy » Authentication Methods—User attribute specifying the list of User Policy-allowed user authentication methods. <p>Using the Admin Console, the administrator creates user accounts with unique usernames. The administrator can assign a User Policy to a user as well as modify the User Policy-related object attributes listed above within a User Policy.</p> <p>The user initializes the value of their credential (password) the first time they log in to an endpoint.</p> <p>When the endpoint receives the User Policy, the endpoint's agent associates the User Policy-related object attributes with the subject. The username and credentials are validated by the authentication server.</p>	
ESM_EAU.2	<p>Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)</p>	<p>Admin Console: Add/Edit Users, Delete Users</p>
	<p>Summary</p> <p>An administrator can create, edit, and delete user accounts. User accounts contain user authentication data.</p>	

SFR	Management functions	Admin role attributes
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Admin Console: Add/Edit Users, Delete Users
	<p>Summary</p> <p>An administrator can create, edit, and delete user accounts. User accounts contain user identities (usernames).</p>	
FAU_SEL.1	Configuration of auditable events	Admin Console: Update System Properties
	<p>Summary</p> <p>An administrator can select the event types audited by the TOE via the Admin Console under System Settings.</p>	
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	Admin Console: Update System Properties
	<p>Summary</p> <p>An administrator on the TOE can configure/select the "event type" of the audit events audited by the agents via the Admin Console under System Settings.</p>	
FAU_STG_EXT.1	Configuration of external audit storage location	Admin Console: Maintain Audit Log
	<p>Summary</p> <p>An administrator can configure the external audit log storage and the external audit server settings (e.g., protocols, IP address, credentials) for the TOE via the Admin Console.</p>	
FIA_AFL.1	Configuration of authentication failure threshold value. Configuration of actions to take when threshold is reached. Execution of restoration to normal state following threshold action (if applicable).	Appliance Console: Super Administrator or Administrator
	<p>Summary</p> <p>For the Admin Console and Appliance Console, the failed login attempts is configurable through the Appliance Console. The action performed is to lock the account for 5 minutes after reaching a configurable number of failed login attempts.</p>	
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	Admin Console: Add/Edit Users
	<p>Summary</p> <p><u>Admin Console</u> There are no default usernames or credentials, but an administrator can modify these subject security attributes at the time of creation or later via the Admin Console.</p> <p>Other subject security attributes are defined in the assigned User Policy. The administrator can modify the assigned User Policy or assign a different User Policy to the user.</p> <p><u>Appliance Console</u></p>	

SFR	Management functions	Admin role attributes
	The Appliance Console Super Administrator account has the Super Administrator role permanently assigned to it. The Administrator account has the Administrator role permanently assigned to it.	
FMT_MOF_EXT.1	<p>Configuration of the behavior of other ESM products</p> <p>Summary See the TSS for FMT_MOF_EXT.1 section 7.1.25 for details.</p>	Admin Console: Assign Computer Policy, Assign User Policy, Create/Edit Computer Policy, Create/Edit User Policy, Maintain Audit Log, Update Computer Policy, Update System Properties
FMT_MSA_EXT.5	<p>Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)</p> <p>Summary See the TSS for FMT_MSA_EXT.5 section 7.1.26 for details.</p>	(Not applicable)
FMT_SMR.1	<p>Management of the users that belong to a particular role</p> <p>Summary All role management is performed through the Admin Console. The Super Administrator role can create, edit, and delete Delegated Administrators roles and assign roles to users. A Delegated Administrator with the <i>Create/Edit Administrator Roles</i> administrator role attribute can create and edit Delegated Administrator roles. A Delegated Administrator with the <i>Delete Administrator Roles</i> administrator role attribute can delete Delegated Administrator roles. A Delegated Administrator with the <i>Add/Edit Users</i> administrator role attribute can assign roles to users. Appliance Console roles cannot be managed.</p>	Admin Console: Create/Edit Administrator Roles, Delete Administrator Roles, Add/Edit Users
FTA_TAB.1	<p>Maintenance of the banner</p> <p>Summary The Admin Console and Appliance Console banners are configurable by an administrator via the Admin Console under "Administrator login message."</p>	Admin Console: Update System Properties
FTP_ITC.1	<p>Configuration of actions that require trusted channel (if applicable)</p> <p>Summary External audit logs: The TOE's external audit log storage SCP connection is managed via the Admin Console in the Audit Records section of the Settings page. The external audit server (syslog) TLS connection is also managed via the Admin Console as well as the Appliance Console.</p>	<p>Admin Console: Maintain Audit Log and/or Update System Properties</p> <p>Appliance Console: Super Administrator or Administrator</p>

SFR	Management functions	Admin role attributes
	<p>To save audit logs on-demand requires the <i>Maintain Audit Log</i> administrator role attribute. To save audit logs periodically requires the <i>Update System Properties</i> administrator role attribute. The Appliance Console is used to configure the low-level aspects of TLS. Because these connections typically only need to be configured once, the need for the Appliance Console is limited to the initialization of the TOE.</p> <p><u>Agent:</u> The network address of the TOE can be configured via the Appliance Console. The TLS versions and ciphersuites used for HTTPS by the Apache HTTP Server when communicating with an agent are non-configurable. The Appliance Console is only used to configure the network address. Because this value typically only needs to be configured once, the need for the Appliance Console is limited to the initialization of the TOE.</p>	
FTP_TRP.1	<p>Configuration of actions that require trusted path (if applicable)</p> <p>Summary <u>Web browser:</u> The network address of the TOE can be configured via the Appliance Console. The TLS versions and ciphersuites used for HTTPS when communicating with the web browser interfaces (i.e., Admin Console and Appliance Console) are fixed. The Appliance Console is only used to configure the network address. Because this connection typically only needs to be configured once, the need for the Appliance Console is limited to the initialization of the TOE.</p>	Appliance Console: Super Administrator or Administrator

7.1.28 FMT_SMR.1 Security roles

SFR Link: [FMT_SMR.1](#)

Admin Console

The Admin Console supports the following roles.

- Super Administrator
- Delegated Administrator

Super Administrator role: There is only one Super Administrator role and it cannot be edited or deleted. The Super Administrator role can perform all administrative operations available from the Admin Console and contains all administrator role attributes. All other administrator roles available from the Admin Console are subordinate to the Super Administrator role.

Delegated Administrator role: Administrator roles subordinate to the Super Administrator role are known as Delegated Administrator roles. The capabilities of a Delegated Administrator role are defined by administrator role attributes, which are assigned to a Delegated Administrator role by either a user with the Super Administrator role or a Delegated Administrator role with the *Create/Edit Administrator Roles* administrator role attribute. Delegated Administrator roles are assigned unique names.

By default, new user accounts have no roles assigned to them. Accounts with no roles assigned are non-administrative accounts.

Appliance Console

The Appliance Console supports the following roles.

- Super Administrator
- Administrator

Super Administrator role: There is one account that is the Super Administrator account and role. The role on this account cannot be modified or deleted. This account can perform all administrative operations available from the Appliance Console. This includes operations such as appliance backup/restore, installation of updates and upgrades, distribution of updates, enterprise data export, reboot/power off, change network settings, and manage system logs. (This list includes features that are not supported and/or not tested in the evaluated configuration.)

Administrator role: There is one account that is the Administrator account and role. The role on this account cannot be modified or deleted. This account performs a subset of the Super Administrative operations available from the Appliance Console. This includes operations such as appliance backup, reboot/power off, change network settings, and manage system logs. (Backup/restore is not a supported feature of the evaluated configuration.)

7.1.29 FPT_APW_EXT.1 Protection of stored credentials

SFR Link: [FPT_APW_EXT.1](#)

The following authentication data are encrypted by the TOE using the database symmetric encryption key to obscure the data prior to storing in the database (non-volatile memory). No interface is provided to view the authentication data in plaintext.

- Admin Console passwords
- Enterprise user passwords
- SSH client password

The following authentication data are obscured using a salted hash, and the obscured data are saved in a password file. No interface is provided to view the passwords in plaintext.

- Appliance Console passwords

7.1.30 FPT_SKP_EXT.1 Protection of secret key parameters

SFR Link: [FPT_SKP_EXT.1](#)

The following data is stored in cleartext on the system. No interface is provided to view this data.

- Database symmetric encryption key used to encrypt/decrypt sensitive data stored in the database
- Apache HTTP Server RSA private key

The following data is encrypted by the TOE using the database symmetric encryption key to obscure the data prior to storing in the database (non-volatile memory).

- SSH client authentication private key

7.1.31 FPT_STM.1 Reliable time stamps

SFR Link: [FPT_STM.1](#)

The TOE's OS provides reliable time stamp capabilities used by the rest of the TOE.

7.1.32 FTA_SSL.3 TSF-initiated termination

SFR Link: [FTA_SSL.3](#)

The TOE terminates the remote sessions of the Admin Console and Appliance Console after an administrator-configurable time interval of inactivity. Once terminated, the administrator must log in again creating a new session. [FMT_SMF.1](#) discusses the configuration of the inactivity time interval.

7.1.33 FTA_SSL.4 User-initiated termination

SFR Link: [FTA_SSL.4](#)

The TOE allows administrators to terminate remote sessions of the Admin Console and Appliance Console via a logout button in both interfaces. When an administrator clicks the logout button, the administrator is logged out and the session terminates.

7.1.34 FTA_TAB.1 Default TOE access banners

SFR Link: [FTA_TAB.1](#)

The TOE displays an administrator-configurable advisory warning message (a.k.a. banner) on the Admin Console and Appliance Console prior to administrator authentication.

7.1.35 FTA_TSE.1 TOE session establishment

SFR Link: [FTA_TSE.1](#)

Administrators can deny session establishment for all Admin Console users, except Super Administrators, based on day, time, and duration. Thus, the attributes are day, time, duration, and user role, where the user role is hardcoded to be all roles except for the Super Administrator role.

The Appliance Console denies session establishment based on usernames. Enterprise users cannot log in to this interface.

7.1.36 FTP_ITC.1 Inter-TSF trusted channel

SFR Link: [FTP_ITC.1](#)

The TOE provides trusted communications between itself and the following IT entities.

- External audit server over TLS
- External audit log storage over SSH
- Agents over HTTPS

External audit server and external audit log storage

The TOE remotely stores audit data to the following locations.

- External audit server (TLS 1.2)
- External audit log storage (SSHv2)

The communication with the external audit server is initiated by the TOE and protected with TLS 1.2. The TLS protocol implementation is provided by OpenSSL. The TOE contains the audit server's CA certificate and uses the audit server's public key to provide assured identification of the remote audit server.

The communication with external audit log storage is initiated by the TOE and protected with SSHv2. The SSH client protocol implementation is provided by Apache SSHD. The TOE has and uses the external SSH server's public key to provide assured identification of external audit log storage.

Agents

The TOE receives inbound connections from the agent over an HTTPS connection. The TOE's HTTPS server supports TLS 1.2. The HTTPS protocol implementation is provided by the Apache HTTP Server. The TLS protocol implementation and cryptographic service provider are provided by Apache NSS.

The TOE does not contact the agent. Instead, the agents contact the TOE each time a user logs in to the endpoint containing an agent and on a configurable, periodic basis called a Refresh Interval as described in [section 1.5.2.1.5](#).

An agent initiates the connection to the TOE to establish a user session, receive policy data, and transmit audit data. The TOE supports the following two methods of assured identification of an agent.

- 1) When a user logs into a managed endpoint, the TOE provides assured identification by validating the user's credentials (username/password) sent by the agent after the TLS connection is established.
- 2) When an agent contacts the TOE for the first time (i.e., enrollment), the TOE sends the agent a unique 128-bit identifier (a.k.a. key) over an HTTPS connection that the agent securely stores. This key allows the TOE to uniquely identify the agent when the agent contacts it. When the agent contacts the TOE when no user is logged into the endpoint (i.e., during a Refresh Interval), the agent uses its unique key to identify itself to the TOE after the HTTPS connection is established.

The latest policy data for the agent is transferred to the TOE each time the agent connects to the TOE, whether it is a user login connection or a Refresh Interval connection. User credentials are transferred to the TOE each time a user logs in to an endpoint containing an agent. Audit data is typically transferred from an agent to the TOE when a user is logged in to an endpoint containing an agent because the agent does not typically generate audit data when there is no user activity.

7.1.37 FTP_TRP.1 Trusted path

SFR Link: [FTP_TRP.1](#)

The TOE supports the following remote web browser-based administrative interfaces:

- Admin Console
- Appliance Console

The web browsers connect to the TOE using HTTPS with TLS 1.2 to protect the communication channels. The connection is protected throughout the entire session, which includes authentication and execution of management functions. The administrative users must log in to the TOE using a username and password, thus, providing assured identification of the user/endpoint.

8 Abbreviations, Terminology, and References

8.1 Abbreviations

AA	Assurance Activity
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CLI	Command Line Interface
DB	Database
DH	Diffie-Hellman
DIT	Data In Transit
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECD	Extended Components Definitions
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ESM	Enterprise Security Management
ESXi	Elastic Sky X Integrated
GCM	Galois/Counter Mode
GUI	Graphical User Interface

HF	Hot Fix
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPM	Imprivata Package Manager
JDK	Java Development Kit
JVM	Java Virtual Machine
JSSE	Java Secure Socket Extension
KeyGen	Key Generation
KeyVer	Key Verification
MAC	Message Authentication Code
MINA	Multipurpose Infrastructure for Network Applications
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSS	Network Security Services
NTP	Network Time Protocol
OE	Operational Environment
OS	Operating System
OTP	One-Time Password
PHP	Hypertext Preprocessor

PKCS	Public-Key Cryptography Standards
PRF	Pseudorandom Function
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SigGen	Signature Generation
SigVer	Signature Verification
SLES	SUSE Linux Enterprise Server
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSPR	Self-Service Password Reset
TD	Technical Decision
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

UI

User Interface

VDI

Virtual Desktop Infrastructure

VM

Virtual Machine

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Agent

The Imprivata Agent is a Windows-based client that executes the authentication and single sign-on policies defined on the Imprivata appliance.

Confirm ID

Imprivata Confirm ID is a technology from Imprivata that provides remote access and multifactor authentication.

HID

Formerly Hughes Identification Devices (HID), HID Global Corporation is a manufacturer of proximity technology such as proximity cards and proximity card readers.

ProveID

Imprivata OneSign ProveID is a technology from Imprivata that can integrate authentication into any device or application.

Refresh Interval

The agent contacts the appliance at the Refresh Interval (i.e., a configurable period of time) to upload audit log data and download policy information.

Secure Walk Away

Imprivata OneSign Secure Walk Away is a Bluetooth-based technology that allows a workstation to detect when a user has walked away from the workstation and has returned to the workstation based on the user's mobile phone Bluetooth signal.

User

Humans or machines interacting with the TOE via the provided user and programmatic interfaces. The term user in this document includes administrators of the TOE unless a specific distinction is made in the text.

VASCO Token

A VASCO token is a small device sold by OneSpan, formerly Vasco Data Security International, Inc., that generates a one-time password (OTP) used for authentication.

Walk-Away Security

Walk-Away Security is a generic OneSign category for technologies like Secure Walk Away and technologies that lock a computer screen after a period of inactivity.

8.3 References

CC	Common Criteria for Information Technology Security Evaluation
	Version 3.1R5
	Date April 2017
	Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
	Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
	Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
CCEVS-PL01	Appropriateness of Language in Security Targets (ST), Assurance Activity Reports (AARs), Product Compliant List (PCL) Entries, Validation Reports (VR), and any other publicly available evaluation documentation
	Date 2014-08-29
	Location https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-1-update2.pdf
CCEVS-TD0042	Removal of Low-level Crypto Failure Audit from PPs
	Date 2018-06-15
	Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0042
CCEVS-TD0055	Move FTA_TAB.1 to Selection-Based Requirement
	Date 2015-07-30
	Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0055
CCEVS-TD0066	Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
	Date 2015-10-08
	Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0066
CCEVS-TD0079	RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
	Date 2018-06-15
	Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0079
CCEVS-TD0573	Update to FCS_COP and FCS_CKM in ESM PPs
	Date 2021-01-29
	Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0573
CCEVS-TD0574	Update to FCS_SSH in ESM PPs
	Date 2021-01-29
	Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0574

CCEVS-TD0576	FTP_ITC and FTP_TRP Updated Date 2021-01-29 Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576
CCEVS-TD0621	Corrections to FCS_TLS_EXT.1 in ESM PPs Date 2022-02-02 Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0621
CCEVS-TD0794	Correction to FCS_SSH_EXT.1.7 Test 2 Date 2023-10-03 Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0794
ESMPMP	Standard Protection Profile for Enterprise Security Management Policy Management Version 2.1 Date 2013-10-24 Location https://www.niap-ccevs.org/MMO/PP/pp_esm_pm_v2.1.pdf
FIPS180-4	Secure Hash Standard (SHS) Date 2015-08-04 Location https://csrc.nist.gov/pubs/fips/180-4/upd1/final
FIPS186-4	Digital Signature Standard (DSS) Date 2013-07-19 Location https://csrc.nist.gov/pubs/fips/186-4/final
FIPS197	Advanced Encryption Standard (AES) Date 2023-05-09 Location https://csrc.nist.gov/pubs/fips/197/final
FIPS198-1	The Keyed-Hash Message Authentication Code (HMAC) Date 2008-07-16 Location https://csrc.nist.gov/pubs/fips/198-1/final
RFC2818	HTTP Over TLS Author(s) E. Rescorla Date 2000-05-01 Location http://www.ietf.org/rfc/rfc2818.txt
RFC3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) Author(s) T. Kivinen, M. Kojo Date 2003-05-01 Location http://www.ietf.org/rfc/rfc3526.txt
RFC4252	The Secure Shell (SSH) Authentication Protocol Author(s) T. Ylonen, C. Lonvick Date 2006-01-01 Location http://www.ietf.org/rfc/rfc4252.txt

RFC4253	The Secure Shell (SSH) Transport Layer Protocol Author(s) T. Ylonen, C. Lonvick Date 2006-01-01 Location http://www.ietf.org/rfc/rfc4253.txt
RFC4254	The Secure Shell (SSH) Connection Protocol Author(s) T. Ylonen, C. Lonvick Date 2006-01-01 Location http://www.ietf.org/rfc/rfc4254.txt
RFC4256	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH) Author(s) F. Cusack, M. Forssen Date 2006-01-01 Location http://www.ietf.org/rfc/rfc4256.txt
RFC4344	The Secure Shell (SSH) Transport Layer Encryption Modes Author(s) M. Bellare, T. Kohno, C. Namprempre Date 2006-01-01 Location http://www.ietf.org/rfc/rfc4344.txt
RFC5246	The Transport Layer Security (TLS) Protocol Version 1.2 Author(s) T. Dierks, E. Rescorla Date 2008-08-01 Location http://www.ietf.org/rfc/rfc5246.txt
RFC6668	SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol Author(s) D. Bider, M. Baushke Date 2012-07-01 Location http://www.ietf.org/rfc/rfc6668.txt
RFC8017	PKCS #1: RSA Cryptography Specifications Version 2.2 Author(s) K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch Date 2016-11-01 Location http://www.ietf.org/rfc/rfc8017.txt
SP800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques Date 2001-12-01 Location https://csrc.nist.gov/pubs/sp/800/38/a/final
SP800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC Date 2007-11-28 Location https://csrc.nist.gov/pubs/sp/800/38/d/final
SP800-56A-Rev3	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography Date 2018-04-16 Location https://csrc.nist.gov/pubs/sp/800/56/a/r3/final

SP800-90A-Rev1 **Recommendation for Random Number Generation Using Deterministic
Random Bit Generators**

Date 2015-06-24

Location <https://csrc.nist.gov/pubs/sp/800/90/a/r1/final>

A Appendixes

A.1 Product Computer Policy

This section contains the complete Computer Policy supported by the product. This section shows how the policy is presented in the Admin Console. Many items in the policy have editable fields that allow an administrator to configure the policy. These editable fields contain the terms: "select", "assignment", and "edit". These terms should not be confused with the "operations" found in [ESM_ACD.1](#). The portions of the Computer Policy tested by this evaluation are shown in [section 1.5.2.1.1.1](#) and are also highlighted in [blue](#) below.

- [General](#)
 - [Shutdown/restart workstation from lock screen \(Select one of: Enable, Disable\)](#)
 - Display name format (Select one of: First and last names; First name, last initial; First name only; Username only)
 - Agent upgrades
 - Agent: (Select one of: Do nothing, Prompt the user to download and install upgrade)
 - ProveID Embedded agent (Select one of: Install the upgrade when idle or on reboot, Install the upgrade only on reboot)
 - Desktop experience
 - Override log in and locking of the Windows workstation (Select one of: Enable, Disable)
 - Authentication
 - If OneSign authentication fails, but Windows authentication succeeds, should the user be allowed to log in to the computer? (Select one of: Yes, No, (Assignment: Specify a list of specific users and/or groups who can))
 - Allow Users to Exit and Disable Agent (Select one of: Yes, No)
 - Accept Kerberos authentication in place of OneSign authentication (Select one of: Enable, Disable)
 - ProveID for interactive authentication
 - Use Confirm ID for Clinical Workflows instead of ProveID for interactive authentication (Select one of: Enable, Disable)
 - Imprivata ID for Hands-Free Authentication (Select one of: Enable, Disable)
 - Card Readers
 - Beep card reader when user taps card (Select one of: Enable, Disable)
 - Select card reader models
 - Enable legacy mode for HID card readers (Select one of: Enable, Disable)
 - Program HID 5x27 card reader configurations (Select one of: Enable, Disable)
 - Smart Card Readers
 - Treat smart card authentications as proximity card authentications (Select one of: Enable, Disable)
 - Agent Logging
 - Enable Agent Logging (Select one of: Yes, No)
 - Agent logging file location (Assignment: Specify filename)

- Maximum file size (Assignment: Specify integer file size in MBs)
- Shared Workstation
 - Notifications
 - Display a temporary greeting notification to the current signed-in user at log-in (Select one of: Enable, Disable)
 - Kiosk Workstations
 - Allow Fast User Switching with Citrix or Terminal Servers (Select one of: Enable, Disable)
 - Automatically shut down Citrix clients when switching users on this workstation? (Select one of: Enable, Disable)
 - Automatically reconnect on session end (Select one of: Enable, Disable)
 - Windows Authentication
 - Authenticate using Windows (Select one of: Enable, Disable)
 - Authenticate using Imprivata (Select one of: Enable, Disable)
 - Multiple Windows Desktops Workstations
 - Enable Multiple Windows Desktops (workstation reboot required) (Select one of: Enable, Disable)
 - Print Connector
 - Enable Imprivata OneSign Print Connector (Select one of: Enable, Disable)
- Walk-Away Security
 - Inactivity detection
 - Keyboard and mouse
 - Lock workstation after (Assignment: Specify time in minutes)
 - Show inactivity warning (Assignment: Specify time in minutes before lock)
 - Imprivata ID
 - Lock workstation after (Assignment: Specify time in minutes)
 - Show inactivity warning (Assignment: Specify time in minutes before lock)
 - Secure Walk Away
 - Lock workstation after (Assignment: Specify time in minutes)
 - Show inactivity warning (Assignment: Specify time in minutes before lock)
 - Automatically re-authenticate user (Assignment: Specify time window in minutes)
 - Lock and warning behavior
 - Lock behavior (Select one of: Visible desktop Obscure desktop)
 - Warning behavior (Select one of: No warning, Notification balloon, Fade to Lock)
 - Advanced settings
 - Ignore mouse movement on transparent lock screens (Select one of: Enable, Disable)
 - Display a notification of the current signed-in user after inactivity (Assignment: Specify time in seconds)
 - Show Secure Walk Away tutorial the first time each user logs in (Select one of: Enable, Disable)

- Secure Walk Away - Imprivata ID sensitivity (Assignment: Specify sensitivity level in values 1 (Near) through 5 (Far))
- Proximity card lock behavior (Select one of: Allow locking and user switching, Allow lock only, Ignore proximity cards)
- Application visible on transparent lock screens (Select one of: None, (Assignment: Specify App name))
- Close the OneSign authentication dialog on transparent lock screens after (Assignment: Specify time in hours, minutes, and seconds)
- Application activity tracking
 - Inactivity target app 1 (Select one of: None, (Assignment: Specify App name))
 - Target app 1 state (Select one of: User is logged off, Application is not running, User is logged off OR Application is not running)
 - Inactivity target app 2 (Select one of: None, (Assignment: Specify App name))
 - Target app 2 state (Select one of: User is logged off, Application is not running, User is logged off OR Application is not running)
 - Lock workstation after (Assignment: Specify time in minutes)
 - Show inactivity warning after (Assignment: Specify time in minutes before lock)
- Virtual Desktops (for thin client endpoints)
 - Users not enabled in OneSign (Select one of: Citrix XenDesktop, MS Remote Desktop Services, VMware Horizon)
 - Persistent applications
 - For each selected app:
 - Launch applications using (Select one of: Windows user account, Anonymous user account)
 - When the computer is Idle (Select one of: Always persist applications, Terminate applications)
 - Persist applications only during specified times (Select one of: Enable, Disable)
 - Assignment: Specify time windows
 - Citrix
 - Citrix XenDesktop
 - Automate access to Citrix XenDesktop (Select one of: Enable, Disable)
 - When a XenDesktop endpoint is locked: (Select one of: Keep the XenDesktop client and user session active, Shutdown the XenDesktop client and disconnect the user session)
 - Citrix XenApp
 - Automate access to Citrix XenApp (Select one of: Enable, Disable)
 - When a XenApp endpoint is locked: (Select one of: Keep the XenApp client and user session active, Shutdown the XenApp client and disconnect the user session)
 - Enable Published Applications (Select one of: Enable, Disable)
 - Microsoft
 - Microsoft Remote Desktop Services - session-based and virtual desktops

- Automate access to session-based and virtual desktops (Select one of: Enable, Disable)
 - When a Remote Desktop endpoint is locked: (Select one of: Keep the Remote Desktop and user session active, Shutdown the Remote Desktop and disconnect the user session)
- Microsoft Remote Desktop Services - RemoteApp
 - Automate access to RemoteApp (Select one of: Enable, Disable)
 - When a Remote Desktop endpoint is locked: (Select one of: Keep the remote applications and user session active, Shutdown the remote applications and disconnect the user session)
- Microsoft Remote Desktop Services - Remote PC
 - Automate access to Remote PC (Select one of: Enable, Disable)
 - When a Remote Desktop endpoint is locked: (Select one of: Keep the Remote Desktop and user session active, Shutdown the Remote Desktop and disconnect the user session)
- VMware
 - VMware Horizon - Desktop
 - Automate access to VMware Horizon (Select one of: Enable, Disable)
 - When a VMware Horizon endpoint is locked: (Select one of: Keep the Horizon client and user session active, Shutdown the Horizon client and disconnect the user session)
 - VMware Horizon - Apps
 - Automate access to VMware Horizon (Select one of: Enable, Disable)
 - When a VMware Horizon endpoint is locked: (Select one of: Keep the VMware Horizon client and user session active, Shutdown the VMware Horizon client and disconnect the user session)
- Citrix or Terminal Server
 - Authenticating generic user or anonymous Citrix XenApp or Terminal Server sessions
 - Authenticate a XenApp or Terminal Server Windows session user based on the identity of the Imprivata user on the client computer (Select one of: The XenApp or Terminal Server Windows session user and Imprivata user are always the same; The XenApp or Terminal Server Windows session user and Imprivata user are not always the same - Use the client computer Imprivata user identity for one of: (Select one of: Anonymous or OneSign Fast User Switching, OneSign Fast User Switching, Anonymous, All sessions))
 - Always trust the Citrix or Terminal Server (Select one of: Enable, Disable)
 - Fast User Switching
 - Endpoints with an installed agent (Select one of: Do not allow remote Fast User Switching, Allow Fast User Switching with the remote server if allowed in computer policy)
 - Endpoints with an installed ProveID Embedded agent (Select one of: Do not allow remote Fast User Switching, Allow Fast User Switching with the remote server if allowed in computer policy)

- Endpoints without an Agent (Select one of: Do not allow remote Fast User Switching; Allow remote Fast User Switching for the specified users: (Assignment: Specify local accounts))
- Fingerprint
 - Fingerprint identification will be suspended after (Assignment: Specify the number of failures) consecutive failures within (Assignment: Specify time in minutes) minutes, for (Assignment: Specify time in minutes) minutes
- Extensions
 - Enable Procedure Code Extension Object? (Select one of: Enable, Disable)
 - When enabled: (Assignment: Specify the OneSign Procedure Code)
 - Enable Managed Exit for MEDITECH Extension Object? (Select one of: Enable, Disable)
 - Enable Carefx Extension Object? (Select one of: Enable, Disable)
- Override and Restrict
 - Single Sign-on
 - Override User Policy? (Select one of: Enable, Disable)
 - Allow offline single sign-on to applications (Select one of: Enable, Disable)
 - Limit offline single sign-on data lifespan: (Assignment: Specify number of days)
 - Display Manage Passwords command in the agent tray menu (Select one of: Enable, Disable)
 - Allow users to bypass single sign-on to access applications (Select one of: Enable, Disable)
 - Challenges
 - Override User Policy?
 - Inactivity lock or hot key behavior (Select one of: Lock computer and suspend OneSign session; Log off user and terminate OneSign session)
 - Challenge users when transitioning from offline to online (Select one of: Always, Wait at least a "specified time period" since their last successful online authentication)
 - Time interval between challenges (Assignment: Specify time in minutes)
 - Desktop Access Authentication Restrictions
 - Restrict user policy (Select one of: Enable, Disable)
 - Allow offline authentication (Select one of: Enable, Disable)
 - Primary factors
 - Password (Select one of: Enable, Disable)
 - Second factors (Requires Confirm ID license)
 - Fingerprint (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN)
 - Proximity Card (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
 - Security Key (Select one of: Enable, Disable)

- Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
- Smart Card or USB token using Active Directory certificate (Select one of: Enable, Disable)
 - Allow temporary use of conditional primary methods (with optional second factor) after initial certificate-based authentication
 - Password (Select one of: Enable, Disable)
 - Built-in proximity card (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
- Smart Card or USB token using external certificate (Select one of: Enable, Disable)
 - Allow temporary use of conditional primary methods (with optional second factor) after initial certificate-based authentication
 - Password (Select one of: Enable, Disable)
 - Built-in proximity card (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
- ID token (Select one of: Enable, Disable)
- VASCO OTP token (Select one of: Enable, Disable)
 - Require password for tokens that do not have a PIN (Select one of: Enable, Disable)
- Answer security questions (Select one of: Enable, Disable)
 - List of security questions (Edit: View/modify/add/delete questions)
 - Select mandatory questions, if any (For each question, select one of: Enable, Disable)
- Spine combined workflow
 - Allow emergency-use single-factor Spine combined workflow (Select one of: Enable, Disable)
- Authentication method options
 - Imprivata ID
 - Allow users to skip enrollment (Select one of: Enable, Disable)
 - If enabled: (Assignment: Specify time in days)
 - After the desktop opens, open the enrollment utility and prompt user to enroll Imprivata ID (Select one of: Enable, Disable)
 - Proximity card
 - Grace period for second authentication factor (Assignment: Specify time in hours and minutes)
 - Security key
 - Grace period for second authentication factor (Assignment: Specify time in hours and minutes)

- Fingerprint
 - Grace period for second authentication factor after fingerprint (Assignment: Specify time in hours and minutes)
 - Number of sequential failed fingerprint authentication attempts before authentication failure (Assignment: Specify number of attempts)
- VASCO OTP token
 - Allow users to enroll VASCO OTP tokens (Select one of: Enable, Disable)
 - If enabled, lock computer if user cancels enrollment (Select one of: Enable, Disable)
 - Allow Offline Authentication with VASCO OTP token (Select one of: Enable, Disable)
 - If allowed, offline data lifespan (Assignment: Specify time in days)
- Smart card using external certificate
 - Allow smart card enrollment and authentication only while certificate is valid (Select one of: Enable, Disable)
- Customization
 - Login customizations
 - Customizable text and banner
 - Show customizable banner
 - Banner background color (Select one of: Color from color palette)
 - Custom message (Assignment: Specify text)
 - Custom cancel button (Assignment: Specify text)
 - Use grayscale start hex (Select one of: Enable, Disable)
 - Login logo and background
 - Show a logo on the lock screen (Select one of: Enable, Disable)
 - Logo (Assignment: Specify picture file to upload)
 - Background (Assignment: Specify picture file to upload)
 - Login authentication prompts
 - Proximity card prompt (Assignment: Specify text)
 - Security key prompt (Assignment: Specify text)
 - Credential prompt (Assignment: Specify text)
 - Proximity card prompt image (Assignment: Specify picture file to upload)
 - Username and password text
 - Username text (Assignment: Specify text)
 - Password text (Assignment: Specify text)
 - Password self-service prompt (Assignment: Specify text)
 - Login UI experience (Select one of: Classic windows login, Imprivata login)
 - Walk-away security
 - Walk-away security notification (Assignment: Specify notification text)

- › Transparent screen lock indicator (Select one of: At the bottom of all displays, At the top of all displays, Do not show indicator)

A.2 Product User Policy

This section contains the complete User Policy supported by the product. This section shows how the policy is presented in the Admin Console. Many items in the policy have editable fields that allow an administrator to configure the policy. These editable fields contain the terms: "select", "assignment", and "edit". These terms should not be confused with the "operations" found in [ESM_ACD.1](#). The portions of the User Policy tested by this evaluation are shown in [section 1.5.2.1.1.2](#) and are also highlighted in blue below.

- [Authentication](#)
 - Licensed options
 - › Fingerprint Identification (Select one of: Enable, Disable)
 - › VASCO OTP Token Authentication (Select one of: Enable, Disable)
 - Walk-away security
 - › Allow Secure Walk Away (Select one of: Enable, Disable)
 - Desktop Access authentication
 - › Allow offline authentication (Select one of: Enable, Disable)
 - › Show greeting notification balloon when users log in (Select one of: Enable, Disable)
 - [Primary factors](#)
 - › [Password \(Select one of: Enable, Disable\)](#)
 - Second factors (Requires Confirm ID license)
 - › Fingerprint (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password; Imprivata PIN)
 - › Proximity Card (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
 - › Security Key (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
 - › Smart Card or USB token using Active Directory certificate (Select one of: Enable, Disable)
 - Allow temporary use of conditional primary methods (with optional second factor) after initial certificate-based authentication
 - Password (Select one of: Enable, Disable)
 - Built-in proximity card (Select one of: Enable, Disable)
 - › Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
 - Allow use of conditional primary methods for: (Assignment: Specify time)
 - › Smart Card or USB token using external certificate (Select one of: Enable, Disable)

- Allow temporary use of conditional primary methods (with optional second factor) after initial certificate-based authentication
 - Password (Select one of: Enable, Disable)
 - Built-in proximity card (Select one of: Enable, Disable)
 - Second factors (Select one of: No second factor, Password, Imprivata PIN, Fingerprint, Fingerprint or Password, Fingerprint or Imprivata PIN)
 - Allow use of conditional primary methods for: (Assignment: Specify time)
- ID token (Select one of: Enable, Disable)
- VASCO OTP token (Select one of: Enable, Disable)
 - Require password for tokens that do not have a PIN (Select one of: Enable, Disable)
- Answer security questions (Select one of: Enable, Disable)
 - Select mandatory questions, if any (Select one of: Enable, Disable)
- Remote access authentication (requires RADIUS server)
 - Password (Select one of: Enable, Disable)
 - VASCO OTP token (Select one of: Enable, Disable)
 - Require password for tokens that do not have a PIN (Select one of: Enable, Disable)
 - ID token (requires external ID token server) (Select one of: Enable, Disable)
- OneSign Anywhere authentication (Requires license)
- Lockout
 - Lock user account after (Assignment: Specify number of failed attempts) consecutive failures within (Assignment: Specify time in minutes) minutes
 - Lock account for (Assignment: Specify time in minutes) minutes
- NIAP access control
 - (Assignment: Specify group names)
 - Allow users to shut down and restart workstation (Select one of: Enable, Disable)
- Authentication method options
 - Security questions
 - List of security questions (Edit: View/modify/add/delete questions)
 - Select mandatory questions, if any (For each question, select one of: Enable, Disable)
 - Number of questions required to enroll (Assignment: Specify the number of questions)
 - Number of questions that must be answered to authenticate (Assignment: Specify the number of questions)
 - Maximum security question logins per month (Assignment: Specify the number of logins)
 - Imprivata ID
 - Allow users to skip enrollment (Select one of: Enable, Disable)
 - If enabled, (Assignment: Specify the number of days)
 - After the desktop opens, open the enrollment utility and prompt user to enroll Imprivata ID (Select one of: Enable, Disable)
 - Allow users to manage Imprivata ID (Select one of: Enable, Disable)

- Imprivata PIN
 - Require users to enroll Imprivata PIN (Select one of: Enable, Disable)
 - PIN length (Assignment: Specify length)
 - Do not allow
 - Repeated digits (1111, 888888) (Select one of: Enable, Disable)
 - Consecutive numbers (1234, 987654) (Select one of: Enable, Disable)
 - PIN that matches the last (Assignment: Specify the number of PINs) PINs created (Select one of: Enable, Disable)
 - PIN expiration
 - Require Imprivata PIN change on expiration (Select one of: Enable, Disable)
 - If enabled, (Assignment: Specify number of days)
 - Imprivata Complex PIN
 - Allow PIN letters, and special characters (Select one of: Enable, Disable)
- Proximity card
 - Specify the number of cards a user is allowed to enroll (Assignment: Specify the number of cards)
 - Grace period for second authentication factor (Assignment: Specify time in hours/minutes)
 - Allow users to enroll a replacement card (Select one of: Enable, Disable)
- Security key
 - Specify the number of security cards a user is allowed to enroll (Assignment: Specify the number of cards)
 - Grace period for second authentication factor (Assignment: Specify time in hours/minutes))
 - Allow users to enroll a replacement security key (Select one of: Enable, Disable)
- Fingerprint
 - Number of sequential failed fingerprint authentication attempts before authentication failure (Assignment: Specify the number of failed attempts)
 - Grace period for second authentication factor (Assignment: Specify time in hours/minutes))
 - Maximum allowed enrolled fingers (Assignment: Specify the number of fingers)
- VASCO OTP token
 - Allow users to enroll VASCO OTP tokens (Select one of: Enable, Disable)
 - Lock computer if user cancels enrollment (Select one of: Enable, Disable)
 - Allow Offline Authentication with VASCO OTP token (Select one of: Enable, Disable)
 - Offline data lifespan (Assignment: Specify the number of days)
- Smart card using external certificate
 - Allow smart card enrollment and authentication only while certificate is valid (Select one of: Enable, Disable)
- Spine Combined Workflow
 - Allow persistence of Spine Combined Workflow session (Select one of: Enable, Disable)

- Grace period for second authentication factor (Assignment: Specify time in hours/minutes))
- Challenges
 - Period of Inactivity before Challenge (Assignment: Specify time in minutes)
 - Time interval between Challenges (Assignment: Specify time in minutes)
 - Hot Key to Lock Workstation or Log off User (Assignment: Specify the keyboard key)
 - At Inactivity Challenge or Pressing Hot Key (Select one of: Lock Workstation/Suspend OneSign Session, Log off User/Terminate OneSign Session)
 - Always challenge users when transitioning from offline to online? (Select one of: Yes; No, don't challenge if it is within (Assignment: Specify time) since their last successful online authentication)
- Self-Service Password/Imprivata PIN Reset
 - Reset options
 - List of security questions (Edit: View/modify/add/delete questions)
 - Select mandatory questions, if any (For each question, select one of: Enable, Disable)
 - Allow users to reset their primary authentication password (Select one of: Enable, Disable)
 - Require users to re-authenticate after resetting their password (Select one of: Enable, Disable)
 - Allow users to reset their Imprivata PIN (Select one of: Enable, Disable)
 - Enroll options
 - Prompt to enroll security questions (Select one of: Prompt and must enroll, Prompt and may delay enrolling, Do not prompt to enroll)
 - Security questions to enroll (Assignment: Specify the number of questions)
 - Authentication with security questions
 - Security questions to authenticate (Assignment: Specify the number of questions)
- Single Sign-On
 - Allow users single sign-on access to applications (Select one of: Enable, Disable)
 - Allow offline single sign-on to applications (Select one of: Enable, Disable)
 - Limit offline single sign-on data lifespan (Select one of: Enable, Disable)
 - Lifespan (Assignment: Specify number of days)
 - Display Manage Passwords command in the agent tray menu (Select one of: Enable, Disable)
 - Allow users to modify and delete application single sign-on credentials (Select one of: Enable, Disable)
 - Show information about managing passwords in notification area balloon tips (Select one of: Enable, Disable)
 - Allow users to reveal application passwords (Select one of: Enable, Disable)
 - Require users to answer security questions to reveal application credentials in SSPR (Select one of: Enable, Disable)
 - List of security questions (Edit: View/modify/add/delete questions)

- Select mandatory questions, if any (For each question, select one of: Enable, Disable)
- Allow users to bypass single sign-on to access applications (Select one of: Enable, Disable)
- Virtual Desktops
 - Enable virtual desktop access automation (Select one of: Enable, Disable)
 - Select automation type (Select one of: Automate access to full VDI desktops, Automate access to applications or published desktops, Automate access to Remote PC)
 - If "Automate access to full VDI desktops," specify the VDI desktops vendor (Select one of: Citrix, Microsoft, VMware) then, on that desktop, launch the following applications: (Select zero or more applications from the list of applications)
 - If "Automate access to applications or published desktops," when a user switches computers, the following application will remain open for them (Select one of: Roam open applications, Roam automatically launched applications)
 - On the endpoint, launch the following applications and/or desktops (Select zero or more applications from the list of applications) then, on all desktops launched, launch the following applications (Select zero or more applications from the list of applications)
 - If "Automate access to Remote PC," on the endpoint, access the following Remote PC (Assignment: Specify Remote PC) then, on all Remote PCs, launch the following applications (Select zero or more applications from the list of applications)