



# Imprivata OneSign Version 7.9 Assurance Activity Report

**Version:** 1.3  
**Date:** 2023-10-06  
**Status:** RELEASED  
**Classification:** Public  
**Filename:** VID11178\_SER\_AAR\_OneSign\_Version\_7.9\_v1.3  
**Product:** Imprivata OneSign Version 7.9  
**Sponsor:** Imprivata, Inc  
**Evaluation Facility:** atsec information security corporation  
**Validation ID:** 11178  
**Validation Body:** NIAP CCEVS  
**Author(s):** Trang Huynh  
**Quality Assurance:** King Ables

This report must not be used to claim product certification, approval, or endorsement by NIAP CCEVS, NVLAP, NIST, or any agency of the Federal Government.

atsec information security corporation  
9130 Jollyville Road, Suite 260  
Austin, TX 78759

Phone: +1 512-615-7300  
[www.atsec.com](http://www.atsec.com)

## Classification Note

### Public Information (public)

This classification level is for information that may be made available to the general public. No specific security procedures are required to protect the confidentiality of this information. Information classified “public” may be freely distributed to anyone inside or outside of atsec.

Information with this classification shall be clearly marked “public”, except that it is not required to mark “public” on printed marketing material obviously intended for publication.

## Revision History

Version	Date	Author(s)	Changes to Previous Revision	Application Notes
1.0	2023-08-02	Trang Huynh	First version	
1.1	2023-09-14	Trang Huynh	Address validator comments	
1.2	2023-10-05	Trang Huynh	Address cert review	
1.3	2023-10-06	King Ables	Add TD0794	

# Table of Contents

<b>1</b>	<b>Evaluation Basis and Documents</b>	<b>7</b>
<b>2</b>	<b>Evaluation Results</b>	<b>8</b>
2.1	CAVP Summary	8
2.2	Vulnerability Analysis	10
2.3	Security Functional Requirements	12
2.3.1	(ESM)	12
2.3.1.1	Access Control Policy Definition (ESM_ACD.1)	12
	TSS Assurance Activities	12
	Guidance Assurance Activities	13
	Test Assurance Activities	13
2.3.1.2	Access Control Policy Transmission (ESM_ACT.1)	14
	TSS Assurance Activities	14
	Guidance Assurance Activities	14
	Test Assurance Activities	14
2.3.1.3	Object Attribute Definition (ESM_ATD.1)	15
	TSS Assurance Activities	15
	Guidance Assurance Activities	16
	Test Assurance Activities	16
2.3.1.4	Subject Attribute Definition (ESM_ATD.2)	17
	TSS Assurance Activities	17
	Guidance Assurance Activities	17
	Test Assurance Activities	18
2.3.1.5	Reliance on Enterprise Authentication (ESM_EAU.2)	18
	TSS Assurance Activities	18
	Guidance Assurance Activities	19
	Test Assurance Activities	20
2.3.1.6	Reliance on Enterprise Authentication (ESM_EID.2)	20
	TSS Assurance Activities	20
	Guidance Assurance Activities	21
	Test Assurance Activities	21
2.3.2	Security audit (FAU)	21
2.3.2.1	Audit Data Generation (FAU_GEN.1)	21
	TSS Assurance Activities	21
	Guidance Assurance Activities	21
	Test Assurance Activities	24
2.3.2.2	Selective Audit (FAU_SEL.1)	25
	TSS Assurance Activities	25
	Guidance Assurance Activities	25
	Test Assurance Activities	25
2.3.2.3	External Selective Audit (FAU_SEL_EXT.1)	26
	TSS Assurance Activities	26
	Guidance Assurance Activities	26
	Test Assurance Activities	27
2.3.2.4	External Audit Trail Storage (FAU_STG_EXT.1)	27
	TSS Assurance Activities	27

Guidance Assurance Activities .....	28
Test Assurance Activities .....	29
2.3.3 Cryptographic support (FCS) .....	29
2.3.3.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1) .....	29
TSS Assurance Activities .....	29
Guidance Assurance Activities .....	30
Test Assurance Activities .....	30
2.3.3.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4) .....	33
TSS Assurance Activities .....	33
Guidance Assurance Activities .....	33
Test Assurance Activities .....	33
2.3.3.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1)) .....	33
TSS Assurance Activities .....	33
Guidance Assurance Activities .....	34
Test Assurance Activities .....	34
2.3.3.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2)) .....	36
TSS Assurance Activities .....	36
Guidance Assurance Activities .....	36
Test Assurance Activities .....	36
2.3.3.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3)) .....	38
TSS Assurance Activities .....	38
Guidance Assurance Activities .....	38
Test Assurance Activities .....	38
2.3.3.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4)) .....	39
TSS Assurance Activities .....	39
Guidance Assurance Activities .....	40
Test Assurance Activities .....	40
2.3.3.7 HTTPS (FCS_HTTPS_EXT.1) .....	40
TSS Assurance Activities .....	40
Guidance Assurance Activities .....	41
Test Assurance Activities .....	41
2.3.3.8 Extended: Cryptographic operation (Random Bit Generation) (FCS_RBG_EXT.1) .....	41
TSS Assurance Activities .....	41
Guidance Assurance Activities .....	42
Test Assurance Activities .....	42
2.3.3.9 SSH (FCS_SSH_EXT.1) .....	43
FCS_SSH_EXT.1.1 .....	43
FCS_SSH_EXT.1.2 .....	44
FCS_SSH_EXT.1.3 .....	45
FCS_SSH_EXT.1.4 .....	46
FCS_SSH_EXT.1.5 .....	47
FCS_SSH_EXT.1.6 .....	48
FCS_SSH_EXT.1.7 .....	49
FCS_SSH_EXT.1.8 .....	50

2.3.3.10	TLS (FCS_TLS_EXT.1)	52
	TSS Assurance Activities	52
	Guidance Assurance Activities	52
	Test Assurance Activities	54
2.3.4	Identification and authentication (FIA)	56
2.3.4.1	Authentication failure handling (FIA_AFL.1)	56
	TSS Assurance Activities	56
	Guidance Assurance Activities	56
	Test Assurance Activities	56
2.3.4.2	User-Subject Binding (FIA_USB.1)	57
	TSS Assurance Activities	57
	Guidance Assurance Activities	57
	Test Assurance Activities	59
2.3.5	Security management (FMT)	59
2.3.5.1	Management of functions behaviour (FMT_MOF.1)	59
	TSS Assurance Activities	59
	Guidance Assurance Activities	60
	Test Assurance Activities	61
2.3.5.2	External Management of Functions Behavior (FMT_MOF_EXT.1)	61
	TSS Assurance Activities	61
	Guidance Assurance Activities	62
	Test Assurance Activities	63
2.3.5.3	Consistent Security Attributes (FMT_MSA_EXT.5)	65
	TSS Assurance Activities	65
	Guidance Assurance Activities	65
	Test Assurance Activities	66
2.3.5.4	Specification of Management Functions (FMT_SMF.1)	66
	TSS Assurance Activities	66
	Guidance Assurance Activities	66
	Test Assurance Activities	71
2.3.5.5	Security Management Roles (FMT_SMR.1)	71
	TSS Assurance Activities	71
	Guidance Assurance Activities	71
	Test Assurance Activities	72
2.3.6	Protection of the TSF (FPT)	73
2.3.6.1	Protection of Stored Credentials (FPT_APW_EXT.1)	73
	TSS Assurance Activities	73
	Guidance Assurance Activities	73
	Test Assurance Activities	73
2.3.6.2	Protection of Secret Key Parameters (FPT_SKP_EXT.1)	74
	TSS Assurance Activities	74
	Guidance Assurance Activities	74
	Test Assurance Activities	75
2.3.6.3	Reliable time stamps (FPT_STM.1)	75
	TSS Assurance Activities	75
	Guidance Assurance Activities	75
	Test Assurance Activities	75

2.3.7 TOE access (FTA)	76
2.3.7.1 TSF-initiated termination (FTA_SSL.3)	76
TSS Assurance Activities	76
Guidance Assurance Activities	76
Test Assurance Activities	76
2.3.7.2 User-initiated termination (FTA_SSL.4)	77
TSS Assurance Activities	77
Guidance Assurance Activities	77
Test Assurance Activities	77
2.3.7.3 TOE Access Banner (FTA_TAB.1)	78
TSS Assurance Activities	78
Guidance Assurance Activities	78
Test Assurance Activities	78
2.3.7.4 TOE Session Establishment (FTA_TSE.1)	79
TSS Assurance Activities	79
Guidance Assurance Activities	79
Test Assurance Activities	80
2.3.8 Trusted path/channels (FTP)	80
2.3.8.1 Inter-TSF Trusted Channel (FTP_ITC.1)	80
TSS Assurance Activities	80
Guidance Assurance Activities	81
Test Assurance Activities	82
2.3.8.2 Trusted path (FTP_TRP.1)	83
TSS Assurance Activities	83
Guidance Assurance Activities	83
Test Assurance Activities	84
2.4 Security Assurance Requirements	85
<b>A Appendixes</b>	<b>86</b>
<b>A.1 References</b>	<b>86</b>
<b>A.2 Glossary</b>	<b>88</b>

## List of Tables

Table 1: SFRs to CAVP certificates for Imprivata OneSign Version 7.9 .....	8
Table 2: Audit record description .....	22
Table 3: Administrator Role Attributes .....	58
Table 4: Access Control Functions .....	62
Table 5: ESM PM PP Management Functions .....	67
Table 6: Imprivata Protocol Support Table .....	81

## 1 Evaluation Basis and Documents

This evaluation is based on the "Common Criteria for Information Technology Security Evaluation" Version 3.1 Revision 5 [CC], the "Common Methodology for Information Technology Security Evaluation" [CEM] and the additional assurance activities defined in the following:

- [ESMPMPV2.1]: Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, 2013-10-24

This evaluation claims Exact Compliance with the above PP.

The following scheme documents and interpretations have been considered:

- [CCEVS-TD0042]: "Removal of Low-level Crypto Failure Audit from PPs", version as of 2018-06-15.
- [CCEVS-TD0055]: "Move FTA\_TAB.1 to Selection-Based Requirement", version as of 2015-07-30.
- [CCEVS-TD0066]: "Clarification of FAU\_STG\_EXT.1 Requirement in ESM PPs", version as of 2015-10-08.
- [CCEVS-TD0079]: "RBG Cryptographic Transitions per NIST SP 800-131A Revision 1", version as of 2018-06-15.
- [CCEVS-TD0573]: "Update to FCS\_COP and FCS\_CKM in ESM PPs", version as of 2021-01-29.
- [CCEVS-TD0574]: "Update to FCS\_SSH in ESM PPs", version as of 2021-01-29.
- [CCEVS-TD0576]: "FTP\_ITC and FTP\_TRP Updated", version as of 2021-01-29.
- [CCEVS-TD0621]: "Corrections to FCS\_TLS\_EXT.1 in ESM PPs", version as of 2022-02-02.
- [CCEVS-TD0794]: "Correction to FCS\_SSH\_EXT.1.7 Test 2", version as of 2023-10-03.

## 2 Evaluation Results

The evaluator work units have been performed, including: evaluator actions and analysis explicitly stated in the CEM; evaluator actions implicitly derived from developer action elements described in the CC Part 3; and evaluator confirmed that requirements for content and presentation of evidence elements described in the CC Part 3 have been met. In addition, the evaluator confirmed that the assurance activities from the claimed PP have been met.

The evaluation was performed by informal analysis of the evidence provided by the sponsor.

**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.

### 2.1 CAVP Summary

**Table 1: SFRs to CAVP certificates for Imprivata OneSign Version 7.9**

SFR	Algorithm	Modes / Other	Implementation	CAVP
FCS_CKM.1	ECDSA KeyGen [FIPS186-4]	P-256, P-384, P-521	Apache NSS	<a href="#">A3233</a>
	ECDSA KeyVer [FIPS186-4]			
	Elliptic curve-based key establishment (KAS-ECC-SSC Sp800-56Ar3) [SP800-56A-Rev3]			
	RSA KeyGen [FIPS186-4]	Moduli: 2048	Bouncy Castle	<a href="#">A3227</a>
	RSA key establishment [RFC8017]	Moduli: 2048	Apache NSS	None
		Modulo: 2048, 3072, 4096	OpenSSL	None
	Finite field-based key establishment [RFC3526]	Diffie-Hellman Group 14	Bouncy Castle	None
FCS_COP.1(1)	AES [FIPS197] [SP800-38A] (CBC)	CBC  128-bit, 256-bit	Apache NSS	<a href="#">A3233</a>



SFR	Algorithm	Modes / Other	Implementation	CAVP
	AES [FIPS197] [SP800-38D] (GCM)	GCM 128-bit, 256-bit		
	AES [FIPS197] [SP800-38A] (CBC)	CBC 128-bit, 256-bit	Bouncy Castle	<a href="#">A3227</a>
	AES [FIPS197] [SP800-38A] (CTR)	CTR 128-bit, 256-bit		
	AES [FIPS197] [SP800-38A] (CBC)	CBC 128-bit, 256-bit	OpenSSL	<a href="#">A899</a>
	AES [FIPS197] [SP800-38D] (GCM)	GCM 128-bit, 256-bit		
FCS_COP.1(2)	RSA SigGen PKCS 1.5 [FIPS186-4]	Moduli: 2048 with SHA-1	Apache NSS	None
		Moduli: 2048 with SHA2-256, SHA2-384, SHA2-512		<a href="#">A3233</a>
	RSA SigGen PKCS 1.5 [FIPS186-4]	Moduli: 2048 with SHA-1	Bouncy Castle	None
	RSA SigVer PKCS 1.5 [FIPS186-4]	Moduli: 2048, 3072, 4096 with SHA-1		<a href="#">A3227</a>

SFR	Algorithm	Modes / Other	Implementation	CAVP
	RSA SigVer PKCS 1.5  [FIPS186-4]	Moduli: 2048, 3072, 4096  using SHA-1, SHA2-256, SHA2-384, SHA2-512	OpenSSL	<a href="#">A899</a>
FCS_COP.1(3)	SHA-1, SHA2-256, SHA2-384, SHA2-512  [FIPS180-4]	160 bits, 256 bits, 384 bits, 512 bits (Byte oriented)	Apache NSS	<a href="#">A3233</a>
	SHA-1, SHA2-256, SHA2-512,  [FIPS180-4]	160 bits, 256 bits, 512 bits (Byte oriented)	Bouncy Castle	<a href="#">A3227</a>
	SHA-1, SHA2-256, SHA2-384, SHA2-512  [FIPS180-4]	160 bits, 256 bits, 384 bits, 512 bits (Byte oriented)	OpenSSL	<a href="#">A899</a>
FCS_COP.1(4)	HMAC [FIPS198-1] [FIPS180-4]	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	Apache NSS	<a href="#">A3233</a>
		HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	Bouncy Castle	<a href="#">A3227</a>
		HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	OpenSSL	<a href="#">A899</a>
FCS_RBG_EXT	Hash_DRBG  [SP800-90A-Rev1]	SHA2-256	Apache NSS	<a href="#">A3233</a>
			Bouncy Castle	<a href="#">A3227</a>
	CTR_DRBG(AES)  [SP800-90A-Rev1]	AES-256	OpenSSL	<a href="#">A899</a>

## 2.2 Vulnerability Analysis

The evaluator searched the following public vulnerability databases to identify relevant CVEs:

- Common Vulnerabilities and Exposures (CVE)

<https://cve.mitre.org/index.html>

The CVE database at MITRE is the largest and most comprehensive source of known vulnerabilities. Other publicly known databases searched by the evaluator were subsets at best, therefore the evaluator used the CVE database as the basis for the analysis.

- Cybersecurity and Infrastructure Security Agency (CISA)  
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- OpenSSL website  
<https://www.openssl.org/news/vulnerabilities.html>  
The evaluator only searched this site for OpenSSL vulnerabilities.

The following search terms were used for CVE searches on the Mitre CVE site above:

- Imprivata OneSign
- Apache HTTP server
- Apache web server
- Apache httpd
- Apache MINA
- Apache Multipurpose Infrastructure for Network Applications
- Apache Network Security Services
- Apache NSS
- Mozilla NSS
- Apache SSHD
- Apache Tomcat
- Bouncy Castle
- BouncyCastle
- Java Virtual Machine
- Java VM
- Java Secure Socket Extension
- Java JSSE
- jvm
- log4j
- OpenJDK
- OpenSSL
- Oracle Database
- Oracle DBMS
- PHP
- spring framework
- spring mvc
- SLES
- SUSE Linux Enterprise Server
- syslog-ng
- TLS 1.2

CVE searches were performed on:

- 2022-11-10
- 2023-02-06

- 2023-06-02
- 2023-07-05
- 2023-07-25
- 2023-08-31
- 2023-09-13

The evaluator found no vulnerabilities that were both present and exploitable in the evaluated configuration.

## 2.3 Security Functional Requirements

### 2.3.1 (ESM)

#### 2.3.1.1 Access Control Policy Definition (ESM\_ACD.1)

##### TSS Assurance Activities

##### Assurance Activity AA-ESM\_ACD.1-ASE-01

*The evaluator shall do the following:*

- *Verify that the TSS identifies one or more compatible Access Control products*
- *Verify that the TSS describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes)*
- *Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the policies the Access Control products are capable of consuming*
- *Verify that the TSS indicates how policies are identified*

##### Summary

Section 7.1.1 ESM\_ACD.1 Access control policy definition of [ST] provides the following description:

- The Access Control products are the Imprivata Agents (a.k.a. agents) each running on a separate Windows 10 OS endpoint.
- The access control policies supported in the evaluated configuration are Computer Policy and User Policy. 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. The User Policy determines the authentication methods available to the user and controls certain endpoints features.
- User authenticating to an endpoint requires both the user and the endpoint enrolled with the TOE and the user must provide the correct credentials known to 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.
- The subjects are users. The objects are various functions on the endpoints controlled by the agent. The operations (along with subjects, subject attributes, objects, and object attributes) are specified in tables 6 through 8 of [ST].
- Each User Policy has a unique User Policy ID and can be assigned to one for more user accounts. Each User Policy can be assigned to one or more user accounts. The TOE maintains the mapping of usernames to User Policy IDs.

- 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.

## Guidance Assurance Activities

### Assurance Activity AA-ESM\_ACD.1-AGD-01

*The evaluator shall review the operational guidance to ensure that it indicates the compatible Access Control product(s) as well as the allowable contents and means of identification of the access control policies that can be defined by the TOE.*

#### Summary

As stated in the [ST][\[1\]](#), the Access Control products are the Imprivata Agents (a.k.a. agents).

The [CCGUIDE][\[1\]](#) provides information about the Agent including installing and setting it up with the TOE appliance.

In the evaluated configuration, the TOE supports the Computer Policy and User Policies.

The [CCGUIDE][\[1\]](#) section *Enterprise Security Management* explains the Computer and User Policies. It states the following:

- 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. Imprivata OneSign 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).
- 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. Imprivata OneSign 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).
- Imprivata supports multiple Computer Policies and User Policies. One Computer Policy is assigned to each managed endpoint and one User Policy is assigned to each user.

## Test Assurance Activities

### Assurance Activity AA-ESM\_ACD.1-ATE-01

*The evaluator shall test this capability by using the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.*

#### Summary

For Test 1, the evaluator created policies that were successfully able to test operations and attributes on a user and computer subject. The object in question is the Windows endpoint where the OneSign Agent is being used for login authentication. The evaluator successfully applied all of the claimed attributes into the two new policies.

The evaluator was able to confirm that all attributes were applied to the two policies successfully. The evaluator was also able to confirm that unique policy identifiers were associated with the two new policies. Both policies were deleted successfully after testing by the superadmin user.

### 2.3.1.2 Access Control Policy Transmission (ESM\_ACT.1)

#### TSS Assurance Activities

##### Assurance Activity AA-ESM\_ACT.1-ASE-01

*The evaluator shall check the TSS and ensure that it summarizes when and how policy data will be transmitted to Access Control products. This includes the ability to specify the product(s) that the policy data will be sent to.*

#### Summary

Section 7.1.2 *ESM\_ACT.1 Access control policy transmission* of [ST] provides the following description:

- 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.
- 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.

#### Guidance Assurance Activities

##### Assurance Activity AA-ESM\_ACT.1-AGD-01

*The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable)*

#### Summary

The [CCGUIDE] section *Computer and Computer Policy* describes how to create and update the Computer Policies. This is done via the TOE's Admin Console. This section states that changes to the computer policy are sent to the Agent at the next refresh interval.

The [CCGUIDE] section *Users and User Policy* describes how to create and update the User Policies. This is done via the TOE's Admin Console. This section states that changes to user policies are sent to the Agent at the next refresh interval.

Instructions for setting the Agent refresh interval is provided in section *Setting the Imprivata Agent Refresh Interval*.

#### Test Assurance Activities

##### Assurance Activity AA-ESM\_ACT.1-ATE-01

*The evaluator shall test this capability by obtaining one or more compatible Access Control products and configuring the TOE to manage them. Then, following the procedures in the operational guidance for both the TOE and the Access Control product, the evaluator shall create a new policy and ensure that the new policy defined in the by the TSF is successfully transmitted to, consumed by, and enforced in an Access Control product, in accordance with the circumstances defined in the SFR. In other words,*

- (a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed;*
- (b) if the selection is completed to transmit periodically, the evaluator shall create the new policy, wait until the periodic interval has passed, and then confirm that the new policy is present in the Access Control component; or*
- (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances.*

*The evaluator shall then make a change to the previously created policy and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component.*

*The evaluator shall repeat this test for a representative sample of Access Control products that can be managed by the TOE. For example, if the TOE provides the ability to manage groups of host-based access control endpoints, the evaluator shall create different groups such that each supported platform is included in at least one group and verify that group members will appropriately consume policies when instructed to do so.*

**Note:** *This testing will likely be performed in conjunction with the testing of ESM\_ACD.1.*

## Summary

Test 1 is to verify the transmission of policies to an authorized Access Control product. This was done by creating both a Computer and a User policy via the Admin Console. These policies were then assigned. An interval refresh of 10 minutes was set on the TOE, and the evaluator waited at least 10 minutes before attempting any actions on the TOE to verify that the policies were transmitted successfully. After signing in, the evaluator waited 10 minutes to verify that the policies automatically updated and transferred to the computer and user.

The evaluator verified that password login was allowed on the Agent, and that reboot was available from the lock screen. These actions were chosen to show one allowance from each policy. After verifying successful authentication and reboot, the policies were then updated. The user policy was updated to not allow any form of authentication, and the computer policy was updated to not allow reboots from the lock screen. The new policies were applied successfully to the user and endpoint after waiting at least 10 minutes for the refresh interval to run. Login was not permitted for the user, and the option to reboot the endpoint was not present.

To test the transmission of a policy upon the agent's first contact with the TOE, the evaluator had to uninstall and reinstall the OneSign agent on the workstation. The TOE behaved as intended, and applied our computer policy to the agent upon first contact.

The evaluator deleted both policies successfully via the Admin Console at the end of testing. For the transmission of policies after authentication on the Agent, please see ESM\_ACD.1 Test 1 and ESM\_ACD.2 Test 1. Test 1 for ESM\_ACT.1 above also shows this action, although its primary purpose is to show the policies being transmitted at a refresh interval of 10 minutes.

### 2.3.1.3 Object Attribute Definition (ESM\_ATD.1)

## TSS Assurance Activities

### Assurance Activity AA-ESM\_ATD.1-ASE-01

*The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.*

## Summary

Section 7.1.3 *ESM\_ATD.1 Object attribute definition* of [ST] refers to section 7.1.1 *ESM\_ACD.1 Access control policy definition*. Section 7.1.1 describes object attributes and their purposes as follows:

- The objects are listed in tables 6, 7, 8 along with their object attributes, if any.
- The endpoint's agent must be registered with the TOE in order for the TOE to manage the capabilities of the endpoint.

## Guidance Assurance Activities

### Assurance Activity AA-ESM\_ATD.1-AGD-01

*The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes.*

## Summary

The evaluator examined section *Computers and Computer Policy* and section *Users and User Policy* within the [CCGUIDE] for information about the objects and the object attributes. Within the section *Computers and Computer Policy*, it states that all attributes for endpoint computers are defined in the Imprivata OneSign user and computer policies, and enforced by the Imprivata agent, installed on the endpoint computer. There, it also states how to configure a computer and/or user policy. Per [ST] tables 6, 7, and 8, the object attributes are:

### Computer Policy

- Session: Inactivity time limit. Guidance is provided in sections *Setting the Imprivata Appliance Console Session Timeout* and section *Setting the Imprivata Admin Console Session Timeout*.
- Shutdown/Restart Workstation Function. Guidance is provided in section *Allowing Users to Restart the Workstation from a Lock Screen*.
- Authentication Function: Computer Policy << Authentication Methods. Guidance is provided in section *Users and User Policy* and section *Offline Authentication Prohibited*.

### User Policy

Per [ST], the User Policy has no object attributes.

### Combined Computer Policy and User Policy

- Authentication Function: Computer Policy << Authentication Methods. Guidance is provided in section *Users and User Policy* and section *Offline Authentication Prohibited*.

## Test Assurance Activities

### Assurance Activity AA-ESM\_ATD.1-ATE-01

*The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.*



## Summary

The evaluator created a new computer policy and applied it to an Access Control product to show that the policy's object attributes were successfully consumed. The default computer policy was first applied to the workstation, and the user was able to reboot the workstation and login via password. After applying the new computer policy, the new restriction of disabling the ability to reboot was successful and the user was not able to reboot. The user was also unable to login via password after the new computer policy took effect.

### 2.3.1.4 Subject Attribute Definition (ESM\_ATD.2)

#### TSS Assurance Activities

##### Assurance Activity AA-ESM\_ATD.2-ASE-01

*The evaluator shall check the TSS to ensure that it describes the subject attributes that are defined by the TOE and the purpose for their definition.*

## Summary

Section 7.1.4 *ESM\_ATD.2 Subject attribute definition* of [ST] refers to section 7.1.1 *ESM\_ACD.1 Access control policy definition*. Section 7.1.1 refers to tables 6 through 8 [ST]. The following subject attributes are described:

- Username. This subject attribute is described throughout section 7.1.1, e.g., within the description of Computer Policy.
- Credentials. This subject attribute is described throughout section 7.1.1, e.g., within the description of Computer Policy.
- User Policy >> Consecutive Failed Login Attempts. This subject attribute is described in section 7.1.1. This function tracks a User-Policy-configurable number of consecutive failed login attempts within the tie window.
- User Policy >> Failure Time Window. This subject attribute is described in section 7.1.1 which is a User Policy-configurable time window for user failed login attempts.
- User Policy >> Lockout time. This subject attribute is described in section 7.1.1 which is a User Policy-configurable amount of time the user is locked out due to failed login attempts.
- User Policy >> Authentication Methods. This subject attribute is described in section 7.1.1. This subject attributes is set in the User Policy to restrict the set of authentication methods available to the users.

#### Guidance Assurance Activities

##### Assurance Activity AA-ESM\_ATD.2-AGD-01

*The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure these attributes.*

## Summary

The evaluator examined section *Computers and Computer Policy* and section *Users and User Policy* within the [CCGUIDE] for information about the subjects and the subject attributes. Within the section *Computers and Computer Policy*, it states that all attributes for endpoint computers are

defined in the Imprivata OneSign user and computer policies, and enforced by the Imprivata agent, installed on the endpoint computer. This section also states how to configure a computer and/or user policy. Per [ST]<sup>1</sup>, the subject attributes are as follows:

- Username. Guidance is provided in section *Create the Super Administrator Account* and section *Administrator Roles (Delegated Administration)*.
- Credentials. Guidance is provided in section *Administrator Roles (Delegated Administration)*.
- User Policy > Consecutive Failed Login Attempts. Guidance is provided in section *User Lockout Policy*
- User Policy > Failure Time Window. Guidance is provided in section *User Lockout Policy*
- User Policy > Lockout time. Guidance is provided in section *Setting the Imprivata Appliance Console Session Timeout* and section *Setting the Imprivata Admin Console Session Timeout*.
- User Policy > Authentication Methods. Guidance is provided in section *Users and User Policy* and section *Offline Authentication Prohibited*.

## Test Assurance Activities

### Assurance Activity AA-ESM\_ATD.2-ATE-01

*The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.*

#### Summary

Test 1 involved the creation of two user policies that defined all attributes listed in [ST]<sup>1</sup> Tables 6, 7, and 8. After creating each policy with the proper attributes configured, the evaluator assigned the policies to our user subjects and logged into the endpoint to verify that both policies were consumed successfully. The evaluator also set the Default Computer Policy to override user authentication after initial login to show that the computer policy can still override authentication methods.

The evaluator performed actions as each user with the intention of showing actions that are allowed and denied by the policies created in Test 1. These actions are allowed and denied correctly in accordance with the policies. The evaluator deleted both user policies successfully after testing.

### 2.3.1.5 Reliance on Enterprise Authentication (ESM\_EAU.2)

#### TSS Assurance Activities

##### Assurance Activity AA-ESM\_EAU.2-ASE-01

*The evaluator shall check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.*

#### Summary

Section 7.1.5 *ESM\_EAU.2 Reliance on enterprise authentication* of [ST]<sup>1</sup> provides the following description:

- Enterprise users (i.e., users on the endpoints) and Admin Console users all authenticate through the same authentication mechanism—the TOE's internal authentication server which uses the TOE's database to the 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.
- The Appliance Console users authenticate via a local password file on the TOE. Only two accounts exist in this password file: Super Administrator and Administrator. In all cases, the user/subject must be identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

## Guidance Assurance Activities

### Assurance Activity AA-ESM\_EAU.2-AGD-01

*The evaluator shall check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to verify that it identifies how these entities are authenticated and what configuration steps must be performed in order to set up the authentication.*

## Summary

### Authentication of interactive users

#### Admin Console

The [CCGUIDE][\[4\]](#), section *Enterprise Security Management*, describes that the TOE maintains user accounts and authentication data in its database. Users of the managed endpoints (agents) and of the Admin Console are validated against this database of users. Section *Security Management* also indicates that the Admin Console supports two types of administrator roles: Super Administrator and Delegated Administrator.

#### Appliance Console

The Appliance Console uses a separate account database/file from the rest of the appliance. This database supports only two password-based accounts: Super Administrator and Administrator. This interface is only used for low-level configuration of the appliance. *Configure the Enterprise Settings* section provides instructions for running the Appliance Configuration Wizard to configure the initial configuration of the appliance. One of the steps during the Appliance Configuration Wizard is for the admin to enter the passwords for both the Super Administrator user and the Administrator user, the only two users of the Appliance Console.

### Authentication of IT entities

#### Authentication of the Agent

Section *More On The Imprivata Agent* states that when the Agent contacts the TOE appliance for the first time (enrollment), the appliance sends the agent a unique 128-bit identifier over an HTTPS connection that the agent secure stores. This key allows the Imprivata appliance to uniquely identify the agent when the agent contacts it. When the agent contacts the appliance when no user is logged into the endpoint (for example, during a refresh interval), the agent uses its unique key to identify itself to the Imprivata appliance after the HTTPS connection is established.

Section *Imprivata Shared Kiosk Workstation Agent* states that when users authenticate to the TOE, the authentication of the username and password entered and the endpoint computer is done at the appliance only. The appliance then returns to the agent an authentication success or failure message only.

### Authentication of the external audit server

The TOE uses SSH with the external audit server. Authentication is via username/password or SSH public key. Instructions to set up SSH are provided in sections *Secure Copy Protocol for Audit File Data* and *SSH Connections From the Imprivata Appliance*

### Authentication of the syslog server

The TOE uses HTTPS with the syslog server. Instructions to set up are provided in section *Remote Syslog Server*.

## Test Assurance Activities

### Assurance Activity AA-ESM\_EAU.2-ATE-01

*The evaluator shall test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.*

*Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).*

### Summary

Test 1: The first test verified that authentication is required on the Appliance Console and the Admin Console before performing any TSF-mediated actions. No TOE modifications can be made prior to authentication. The evaluator confirmed that access to the TSFIs were denied upon entering incorrect credentials, and that the required audit logs were captured by the TOE.

Test 2: Positive testing was not required for this SFR, as this is assumed in [ESMPMPP] to be tested by other requirements.

## 2.3.1.6 Reliance on Enterprise Authentication (ESM\_EID.2)

### TSS Assurance Activities

#### Assurance Activity AA-ESM\_EID.2-ASE-01

*This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM\_EAU.2.*

### Summary

Section 7.1.6 *ESM\_EID.2 Reliance on enterprise identification* of [ST] provides the following statement: The information for this TSS has been included in the TSS for ESM\_EAU.2 section 7.1.5. Section 7.1.5 provides the following description:

- Enterprise users (i.e., users on the endpoints) and Admin Console users authenticate through the same 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.
- The Appliance Console users authenticate via a local password file on the TOE. Only two accounts exist in this password file: Super Administrator and Administrator. These are not 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.

## Guidance Assurance Activities

### Assurance Activity AA-ESM\_EID.2-AGD-01

*This functionality —for both interactive users and authorized IT entities— is verified concurrently with ESM\_EAU.2.*

#### Summary

The evaluator performed this assurance activity in conjunction with ESM\_EAU.2 AA-ESM\_EAU.2-AGD-01.

## Test Assurance Activities

### Assurance Activity AA-ESM\_EID.2-ATE-01

*This functionality —for both interactive users and authorized IT entities— is verified concurrently with ESM\_EAU.2.*

#### Summary

No separate testing required, as this functionality - for both interactive users and authorized IT entities - is verified concurrently with ESM\_EAU.2.

## 2.3.2 Security audit (FAU)

### 2.3.2.1 Audit Data Generation (FAU\_GEN.1)

## TSS Assurance Activities

### Assurance Activity AA-FAU\_GEN.1-ASE-01

*The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.*

#### Summary

Section 7.1.7 FAU\_GEN.1 Audit data generation of [ST] provides the following description:

- The TOE generates audit records for the events specified in Table 9 "Auditable events" as well as audit records for the audit trail startup and shutdown events. The evaluator located Table 9, which is provided in the FAU\_GEN.1 SFR itself. Thus, all applicable auditable events.
- Per section 7.1.7, besides containing the necessary additional information specified in Table 9, each audit record contains the date and time of the event, type of event, subject identity (if applicable), and outcome.

## Guidance Assurance Activities

### Assurance Activity AA-FAU\_GEN.1-AGD-01

*The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record.*

*Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU\_GEN 1.2, and the additional information specified in Table 3 of [ESMPMPV2.1].*

The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD\_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.

## Summary

Section *Information in the Audit Log* of [CCGUIDE] contains a list of auditable events corresponding to those identified in [ST] section 6.1.2.1 *Audit data generation (FAU\_GEN.1)*, Table 9 *Auditable events*, along with a description of the audit record format. In addition, the section below the audit table lists the 16 possible fields provided in the audit logs such as username, timestamp, type of activity, authentication method, etc. which the evaluator found to be self-explanatory. The following table identifies the audit events claimed in the FAU\_GEN.1 requirements of [ST] and the corresponding audit samples described in section *Information in the Audit Logs* of [CCGUIDE]. In constructing this table, the evaluator determined the audit records contain the possible fields mentioned above.

**Table 2: Audit record description**

SFR	Auditable Events	Additional Audit Record Contents	Audit record description
FAU_GEN.1	Start-up of the audit functions		The provided audit records shows the audit functions starting up.
FAU_GEN.1	Shutdown of the audit functions		The provided audit records shows the audit functions shutting down.
ESM_ACD.1	Creation or modification of policy	Unique policy identifier	Added User Policy, Modified User Policy, Deleted User Policy  The provided audit records contain fields including user ID, the action (eg., added user policy 'New Policy'), timestamp, and status.
ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy	The provided audit shows the new Computer Policy has been applied.
ESM_ATD.1	Definition of object attributes	Identification of the attribute defined	The provided audit record shows successful assignment of User Policy and its attributes.
ESM_ATD.1	Association of attributes with objects	Identification of the object and the attribute	The provided audit record shows successful association of a computer policy and its attributes.

SFR	Auditable Events	Additional Audit Record Contents	Audit record description
ESM_ATD.2	Definition of subject attributes	Identification of the attribute defined	The provided audit records show successful assignment of the user (e.g., Suepr Administrator) and their attributes.
ESM_ATD.2	Association of attributes with subjects	Identification of the subject and the attribute	The provided audit record shows successful assignment of the user (e.g., testuser) and their attributes
ESM_EAU.2	All use of the authentication mechanism	None	The provided audit records provided cover user login, agent login, agent lock, exit, and inactivity lock.
FAU_SEL_EXT.1	All modifications to audit configuration	None	The provided audit record shows changes to the audit setting.
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server (including external audit log storage)	Identification of audit server (including external audit log storage)	The provided audit record shows successful and failed connections for the syslog server.
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)	The provided audit record shows successful and failed HTTPS connections with the Agent.
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)	The provided audit record shows successful and failed connections with teh external audit server.
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)	The provided audit record shows failed HTTPS connection. Necessary fields are included in the audit record such as user ID, status.
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached	The provided audit record shows a user reaching lockout threshold and the account is locked.
FMT_MOF.1	All modifications of TSF function behavior	None	No explicit audit records provided. The evalutaor found audit records for management functions are provided via audit records of other related SFRs, e.g., FTP_ITC.1



SFR	Auditable Events	Additional Audit Record Contents	Audit record description
FMT_SMF.1	Use of the management functions	Management function performed	No explicit audit records provided. The evaluator found audit records for management functions are provided via audit records of other related SFRs, e.g., ESM_ATD.1.
FMT_SMR.1	Modifications to the members of the management roles	None	The provided audit records cover changing user roles.
FTA_SSL.3	All session termination events	None	The provided audit records cover different user termination events including successful user logout.
FTA_SSL.4	All session termination events	None	The provided audit records cover different user termination events including user session timeout.
FTA_TSE.1	Denial of session establishment	None	The provided audit records cover system logout, attempted login, manual account unlock,
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel	The provided audit records cover HTTPS and SSH connections.
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available	The provided audit records show user logins via consoles.

The evaluator reviewed the [CCGUIDE] in accordance with AGD\_OPE.1-2 to determine the administrative interfaces that permit configuration of the TOE. From AGD\_OPE.1-2, the methodology used to do this is described and outlined. The evaluator determined that audit-related configurations is performed via the Admin Console and guidance to perform configurations are provided throughout section *Server Configurations*. Using this approach, the evaluator determined that the [CCGUIDE] adequately correlates each of the security relevant administrative interfaces with their corresponding audit events and that the appropriate information is recorded for each of the recorded events.

## Test Assurance Activities

### Assurance Activity AA-FAU\_GEN.1-ATE-01

*The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.*



*This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.*

## Summary

The evaluator triggered all events listed in Table 9 of the [ST] and administrative actions throughout the testing. Relevant logs for administrative actions were gathered and recorded in FMT\_MOF.1. All relevant logs were gathered via the Admin and Appliance Console TSFIs for each test case, and the logs contained the required information.

### 2.3.2.2 Selective Audit (FAU\_SEL.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FAU\_SEL.1-ASE-01

*The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to have selective auditing and that it summarizes the mechanism(s) by which auditable events are selected for auditing.*

## Summary

Section 7.1.8 FAU\_SEL.1 Selective audit of [ST] states that an 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.

#### Guidance Assurance Activities

##### Assurance Activity AA-FAU\_SEL.1-AGD-01

*The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.*

## Summary

In section *Auditing* of the [CCGUIDE], it mentions that an administrator can select events to be audited by Imprivata based on the event type. Section *Manage Audit Records* provides instructions for excluding audit event types from logging. The section provides the steps for managing the audit records.

#### Test Assurance Activities

##### Assurance Activity AA-FAU\_SEL.1-ATE-01

*The evaluator shall test this capability by using all allowable vectors that are defined in FMT\_MOF.1 to configure the TOE in the following manners:*

- All selectable auditable events enabled
- All selectable auditable events disabled
- Some selectable auditable events enabled

*For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded.*

## Summary

Testing for this SFR was performed with the intention of filtering TOE audit logs based off of event types.

The evaluator verified that the administrator had the ability to modify selectable auditable events and decide which audit events are recorded. This was done by first unchecking all of the event types, which added the logs to the Deny List successfully. Login and logout actions were then performed by the evaluator to verify that these logs were not recorded.

The evaluator then chose a select few event types to filter for, including Administrative Login but not logout. The logs that were selected were then removed from the Deny List successfully. Login and logout actions were then performed by the evaluator to verify that only the login attempts were recorded.

After selecting all log types, there were no log events on the Deny List. This included recording Administrative Logout events. Login and logout actions were then performed by the evaluator to verify all login and logout attempts were recorded. All functions were executed via the Admin Console TSFI.

### 2.3.2.3 External Selective Audit (FAU\_SEL\_EXT.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FAU\_SEL\_EXT.1-ASE-01

*The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to configure selective auditing for an Access Control product and that it summarizes the mechanism(s) by which auditable events are selected for auditing.*

## Summary

Section 7.1.9 FAU\_SEL\_EXT.1 External selective audit of [ST] provides the following description:

- 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.
- This section also refers to Table 21 (entry FAU\_SEL\_EXT.1) of the TSS for FMT\_SMF.1 for additional information. The evaluator examined Table 21, which provides a summary of the available management functions including configuration of auditable events.

#### Guidance Assurance Activities

##### Assurance Activity AA-FAU\_SEL\_EXT.1-AGD-01

*The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.*

## Summary

The [CCGUIDE] sections *Manage Audit Records* and *Audit Record Maintenance* provide guidance on how the administrators can select auditable events to be audited. This is performed via the Admin Console. From testing, the evaluator confirmed that all of the selections identified in the Security Target are met.

## Test Assurance Activities

### Assurance Activity AA-FAU\_SEL\_EXT.1-ATE-01

*The evaluator shall test this capability by configuring a compatible Access Control product to have:*

- All selectable auditable events enabled
- All selectable auditable events disabled
- Some selectable auditable events enabled

*For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded by the Access Control product.*

*If this SFR is iterated, the evaluator shall repeat these activities for each iteration of the SFR, substituting the appropriate external entity for "Access Control product" where appropriate.*

#### Summary

For Test 1, the evaluator verified that the administrator was able to modify which logs were audited for an Access Control product. The test went through the management function of enabling all logs, disabling all logs, and enabling select logs based off of event type. The evaluator used various event types to show the logs successfully being filtered. If the event type was on the Log Deny list, the event was shown to not be recorded.

The TOE logged these changes successfully, and audit logs for our OneSign Agent were recorded accurately based on the filtered events set by the evaluator.

### 2.3.2.4 External Audit Trail Storage (FAU\_STG\_EXT.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FAU\_STG\_EXT.1-ASE-01

*The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.*

*If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented.*

#### Summary

Section 7.1.10 FAU\_STG\_EXT.1 External audit trail storage of [ST] provides the following description:

- The TOE uses two separate local auditing mechanisms to record different events as listed in Table 13 "Audit storage mechanisms" and outlined below.
  1. TOE's local data - audit records are transferred to an external audit log storage via an SSH channel.
  2. local syslog file - audit records are transferred to an external audit server (syslog) via a TLS channel.

Both SSH and TLS are defined in FTP\_ITC.1. Also, all audit records are protected from unauthorized deletion and modification by only allowing administrators with the appropriate administrator role attributes to access the audit records.

- Audit record data is also not lost. External audit log storage can be configured to transfer audit records either periodically or on-demand. For the periodic option, the TOE automatically transfers audit records in log files to the external audit log storage at administrator-defined intervals. In the case of a connection failure or the external storage is unavailable, the TOE attempts to transfer the audit records at the next interval. For the on-demand option, the TOE transfer audit records in log files to the external audit log storage at the administrator's request. In the case of a connection failure or the external storage is unavailable, the TOE and the administrator must reattempt the transfer.
- 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.

## Guidance Assurance Activities

### Assurance Activity AA-FAU\_STG\_EXT.1-AGD-01

*The evaluator shall check the operational and preparatory guidance in order to determine that they describe how to configure and use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.*

*If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented.*

## Summary

Section *Sever Configurations* subsection *Auditing Mechanisms* details of [CCGUIDE] the two audit mechanisms outlined by the [ST], which are the external audit log storage and the external audit server (syslog). 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.

Guidance on the syslog server is provided in section *Remote Syslog Server* including instructions to set up TLS.

Guidance on the external audit log storage is provided in sections *Secure Copy Protocol for Audit File Data*, *SSH Connections From The Imprivata Appliance*.

In addition, section *External Audit Log Storage* states the following:

- The external audit log storage mechanism can be configured to transfer audit records two different ways: periodically and on-demand. When configured for periodic transfers, Imprivata OneSign 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, Imprivata OneSign retains the log files and attempts to transfer them at the next interval. When configured for on-demand transfers, Imprivata OneSign transfers audit records in log files to the external audit log storage at the request of the administrator.

Furthermore, section *External audit server (syslog)* states the following:

- 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 reestablished, only audit records generated after the reestablishment are sent to the external audit server. No alert or notification is provided to the administrator regarding these lost audit records.
- Imprivata OneSign recovers from such an outage as quickly as possible, and the Administrator can make no specific configuration changes that will improve upon the recovery time.

## Test Assurance Activities

### Assurance Activity AA-FAU\_STG\_EXT.1-ATE-01

*If the ST claims that the TOE does audit reconciliation, then the following test must be run.*

*The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU\_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP\_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.*

#### Summary

NOTE that the ST does not claim audit reconciliation, but only re-establishment of the connection. This is also noted in the [DTR].

Test 1 is to verify the connection and successful transfer of audit data to both a syslog server and an external audit log storage server. Connections were established by the evaluator to transmit audit data externally to a syslog server and an SCP server. The evaluator verified that audit data was successfully generated and saved both locally on the TOE and externally on the server in question. All required audit logs were successfully generated by the TOE.

Test 2 was also shown in Test 1 above. The evaluator confirmed that each connection was established successfully using a trusted channel defined in FTP\_ITC.1.

Test 3 is tested in ESM\_EAU.2 Test 1 and FIA\_USB.1 Tests 1, 2, and 3 by showing that TSF access is based on role and prior admin authentication. Only Administrator users are able to access the TOE Admin and Appliance UIs.

## 2.3.3 Cryptographic support (FCS)

### 2.3.3.1 Cryptographic Key Generation (for asymmetric keys) (FCS\_CKM.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FCS\_CKM.1-ASE-01

*The evaluator shall ensure that the TSS identifies the key sizes and key establishment schemes supported by the TOE. The evaluator shall examine the TSS to verify that it identifies the usage for each scheme.*

#### Summary

Section 7.1.11 *FCS\_CKM.1 Cryptographic key generation (for asymmetric keys)* provides Table 14: Asymmetric key generation, verification, and establishment algorithms it identifies the following key establishment schemes supported by the TOE including their key sizes and usage.

- RSA key establishment with modulo 2048 provided by the Apache NSS cryptographic module for the HTTPS server
- Elliptic curve-based key establishment (KAS-ECC-SSC Sp800-56Ar3) with curves P-256, P-384, P-521 provided by the Apache NSS cryptographic module for the HTTPS server
- Finite field-based key establishment with Diffie-Hellman Group 14 provided by Bouncy Castle for SSH client authentication and key pair generation
- RSA key establishment with moduli 2048, 3072, 4096 provided by OpenSSL for the TLS client

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_CKM.1-AGD-01

*The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s) and key sizes for all uses defined in this PP.*

#### Summary

For HTTPS, SSH, and TLS, the evaluator examined section *Protection of Imprivata Security Functions* of [CCGUIDE], which states Imprivata provides no interface to view pre-shared keys, symmetric keys, and private keys.

Also, section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST.

In addition, the evaluator examined section *Server Configurations* of [CCGUIDE], which provides several highlighted information notes that state the following:

- Beneath subsection *Configure SCP for Audit Records*, the note states,  
"*The SSH Public Key authentication method cannot be changed. The algorithms for the SSH protocol cannot be changed;*"
- Within the section *Remote Syslog Server*, the note states,  
"*TLS, Bouncy Castle, and NSS are the only cryptography engines used by Imprivata OneSign. Imprivata OneSign administrators cannot configure this. Any other cryptography engines are prohibited in the Common Criteria evaluated configuration.*"

Thus, the evaluator determined that the administrator does not need to configure the TOE to use the key generation scheme and key size. The cryptographic keys are generated along with the TLS client certificates. The use of the key establishment schemes is done automatically.

## Test Assurance Activities

### Assurance Activity AA-FCS\_CKM.1-ATE-01

*The evaluator shall verify the implementation of the key establishment schemes supported by the TOE using the applicable tests below.*

#### **SP800-56A Key Establishment Schemes**



The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value Z) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag.

#### **Function Test**

The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested.

The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information (OtherInfo) and TOE id fields.

If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret.

The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values.

If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm.

#### **Validity Test**

The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the OtherInfo and TOE id fields.

The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the OtherInfo field, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).

The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.

#### **SP800-56B Key Establishment Schemes**

The evaluator shall verify that the TSS describes whether the TOE acts as a sender, a recipient, or both for RSA-based key establishment schemes.

If the TOE acts as a sender, the following evaluation activity shall be performed to ensure the proper operation of every TOE supported combination of RSA-based key establishment scheme:

To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each combination of supported key establishment scheme and its options (with or without key confirmation if supported, for each supported key confirmation MAC function if key confirmation is supported, and for each supported mask generation function if KTS-OAEP is supported), the tester shall generate 10 sets of test vectors. Each test vector shall include the RSA public key, the plaintext keying material, any additional input parameters if applicable, the MacKey and MacTag if key confirmation is incorporated, and the outputted ciphertext. For each test vector, the evaluator shall perform a key establishment encryption operation on the TOE with the same inputs (in cases where key confirmation is incorporated, the test shall use the MacKey from the test vector instead of the randomly generated MacKey used in normal operation) and ensure that the outputted ciphertext is equivalent to the ciphertext in the test vector.

If the TOE acts as a receiver, the following evaluation activities shall be performed to ensure the proper operation of every TOE supported combination of RSA-based key establishment scheme:

To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each combination of supported key establishment scheme and its options (with or without key confirmation if supported, for each supported key confirmation MAC function if key confirmation is supported, and for each supported mask generation function if KTS-OAEP is supported), the tester shall generate 10 sets of test vectors. Each test vector shall include the RSA private key, the plaintext keying material (KeyData), any additional input parameters if applicable, the MacTag in cases where key confirmation is incorporated, and the outputted ciphertext. For each test vector, the evaluator shall perform the key establishment decryption operation on the TOE and ensure that the outputted plaintext keying material (KeyData) is equivalent to the plaintext keying material in the test vector. In cases where key confirmation is incorporated, the evaluator shall perform the key confirmation steps and ensure that the outputted MacTag is equivalent to the MacTag in the test vector.

The evaluator shall ensure that the TSS describes how the TOE handles decryption errors. In accordance with NIST Special Publication 800-56B, the TOE must not reveal the particular error that occurred, either through the contents of any outputted or logged error message or through timing variations. If KTS-OAEP is supported, the evaluator shall create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.2.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each. If KTS-KEM-KWS is supported, the evaluator shall create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.3.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each.

#### **RSA-based key establishment**

The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1\_5 by using a known good implementation for each protocol selected in FTP\_ITC.1 and FTP\_TRP.1 that uses RSAES-PKCS1-v1\_5.

#### **FFC Schemes using Diffie-Hellman Group 14**

The evaluator shall verify the correctness of the TSF's implementation of Diffie-Hellman group 14 by using a known good implementation for each protocol selected in FTP\_ITC.1 and FTP\_TRP.1 that uses Diffie-Hellman group 14.

#### **FFC Schemes using "safe-prime" groups**

The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP\_ITC.1 and FTP\_TRP.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.

## **Summary**

The evaluator verified the implementation of the key establishment schemes supported by the TOE using either the Cryptographic Algorithm Validation Program (CAVP), or the applicable tests included in this assurance activity.

### **Elliptic curve-based key establishment (KAS-ECC-SSC Sp800-56Ar3) with curves P-256, P-384, P-521**

(provided by the Apache NSS cryptographic module for the HTTPS server)

This key establishment method was performed using the CAVP in accordance with the CAVP test procedures. The results have been validated by the CAVP and the certificate information is provided in section 2.1, "CAVP Summary," in the Assurance Activity Report (AAR).

### **RSA key establishment with moduli 2048**

(provided by the Apache NSS cryptographic module for the HTTPS server)

### **RSA key establishment with moduli 2048, 3072, 4096**

(provided by OpenSSL for the TLS client)

These key establishing methods were tested following the requirements of this assurance activity. The CAVP does not cover RSAES-PKCS1-v1\_5 (i.e. RSA encryption/decryption using PKCS#1v1.5 padding).



The evaluator tested this key establishment method using a TLS connection between the TOE and a known good implementation of the TLS protocol, forcing the selection of a cipher suite that used RSA key exchange. The evaluator verified that in all cases the TLS handshake was successful.

**Finite field-based key establishment with Diffie-Hellman Group 14**  
(provided by Bouncy Castle for SSH client authentication)

This key establishing method was tested following the requirements of this assurance activity. The CAVP does not fully cover Diffie-Hellman key agreement.

The evaluator tested this key establishment method using a SSH connection between the TOE and a known good implementation of the SSH protocol, forcing the selection of DH group 14 used as the key exchange method. The evaluator verified that in all cases the TLS handshake was successful.

Notice that all key establishment schemes have been also tested implicitly during the execution of the rest of the test suite, especially in the scope of FTP\_ITC.1 and FTP\_TRP.1.

### 2.3.3.2 Cryptographic Key Zeroization (FCS\_CKM\_EXT.4)

#### TSS Assurance Activities

##### Assurance Activity AA-FCS\_CKM\_EXT.4-ASE-01

*The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").*

#### Summary

Section 7.1.12 *fcs\_cop.1.4 Cryptographic key zeroization* of [ST] describes key destruction. It provides Table 15 "Key destruction" outlining the secret keys, private keys, and critical security parameters, the storage location type, when the values are destroyed, and the destruction method. For example, the AES session keys used by the TLS client stored in volatile memory are zeroized via single overwrite with zeros after session completion. The evaluator found the information to be sufficiently described. With the exception of the database symmetric encryption (stored in both volatile and non-volatile memories) used by the Apache HTTPS server, all other key materials and CSPs are zeroized via single overwrite with zeros.

#### Guidance Assurance Activities

No assurance activities defined.

#### Test Assurance Activities

No assurance activities defined.

### 2.3.3.3 Cryptographic Operation (for data encryption/decryption) (FCS\_COP.1(1))

#### TSS Assurance Activities

No assurance activities defined.

## Guidance Assurance Activities

No assurance activities defined.

## Test Assurance Activities

### Assurance Activity AA-FCS\_COP.1-1-ATE-01

The evaluator shall perform all of the following tests for each algorithm implemented by the TSF and used to satisfy the requirements of this PP:

#### AES-CBC Known Answer Tests

There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

- KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.
- KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.
- KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key  $i$  in each set shall have the leftmost  $i$  bits be ones and the rightmost  $N-i$  bits be zeros, for  $i$  in  $[1, N]$ . To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key  $i$  in each set shall have the leftmost  $i$  bits be ones and the rightmost  $N-i$  bits be zeros, for  $i$  in  $[1, N]$ . The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.
- KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value  $i$  in each set shall have the leftmost  $i$  bits be ones and the rightmost  $128-i$  bits be zeros, for  $i$  in  $[1, 128]$ .

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

#### AES-CBC Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an  $i$ -block message where  $1 < i \leq 10$ . The evaluator shall choose a key, an IV and plaintext message of length  $i$  blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation. The evaluator shall also test the decrypt functionality for each mode by decrypting an  $i$ -block message where  $1 < i \leq 10$ . The evaluator shall choose a key, an IV and a ciphertext message of length  $i$  blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation. AES-CBC Monte Carlo Tests The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:

```
# Input: PT, IV, Key
for i = 1 to 1000:
  if i == 1:
    CT[1] = AES-CBC-Encrypt(Key, IV, PT)
    PT = IV
```

```
else:  
    CT[i] = AES-CBC-Encrypt(Key, PT)  
    PT = CT[i-1]
```

The ciphertext computed in the 1000<sup>th</sup> iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

#### **AES-GCM Monte Carlo Tests**

The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

- 128 bit and 256 bit keys
- Two plaintext lengths. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported. Three AAD lengths. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.
- Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

#### **AES-CTR Known Answer Tests**

The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. Since the Counter Mode does not specify the counter that is used, it is not possible to implement an automated test for this mode. The generation and management of the counter is tested through FCS\_SSH\*\_EXT.1.4. If CBC and/or GCM are selected in FCS\_COP.1/DataEncryption, the test activities for those modes sufficiently demonstrate the correctness of the AES algorithm. If CTR is the only selection in FCS\_COP.1/DataEncryption, the AES-CBC Known Answer Test, AESGCM Known Answer Test, or the following test shall be performed (all of these tests demonstrate the correctness of the AES algorithm):

There are four Known Answer Tests (KATs) described below to test a basic AES encryption operation (AES-ECB mode). For all KATs, the plaintext, IV, and ciphertext values shall be 128-bit blocks. The results from each test may either be obtained by the validator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

- KAT-1 To test the encrypt functionality, the evaluator shall supply a set of 5 plaintext values for each selected key size and obtain the ciphertext value that results from encryption of the given plaintext using a key value of all zeros.
- KAT-2 To test the encrypt functionality, the evaluator shall supply a set of 5 key values for each selected key size and obtain the ciphertext value that results from encryption of an all zeros plaintext using the given key value.
- KAT-3 To test the encrypt functionality, the evaluator shall supply a set of key values for each selected key size as described below and obtain the ciphertext values that result from AES encryption of an all zeros plaintext using the given key values. A set of 128 128-bit keys, a set of 192 192-bit keys, and/or a set of 256 256-bit keys. Key<sub>i</sub> in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1, N].
- KAT-4 To test the encrypt functionality, the evaluator shall supply the set of 128 plaintext values described below and obtain the ciphertext values that result from encryption of the given plaintext using each selected key size with a key value of all zeros (e.g. 256 ciphertext values will be generated if 128 bits and 256 bits are selected and 384 ciphertext values will be generated if all key sizes are selected). Plaintext value i in each set shall have the leftmost bits be ones and the rightmost 128-i bits be zeros, for i in [1, 128]. AES-CTR Multi-Block Message Test 114 The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 less-than i

less-than-or-equal to 10 (test shall be performed using AES-ECB mode). For each  $i$  the evaluator shall choose a key and plaintext message of length  $i$  blocks and encrypt the message, using the mode to be tested, with the chosen key. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key using a known good implementation. The evaluator shall perform this test using each selected keysize.

#### **AES-CTR Monte-Carlo Test**

The evaluator shall test the encrypt functionality using 100 plaintext/key pairs. The plaintext values shall be 128-bit blocks. For each pair, 1000 iterations shall be run as follows: # Input: PT, Key for  $i = 1$  to 1000:  $CT[i] = \text{AES-ECB-Encrypt}(\text{Key}, \text{PT})$   $PT = CT[i]$

The ciphertext computed in the 1000<sup>th</sup> iteration is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation. The evaluator shall perform this test using each selected keysize.

There is no need to test the decryption engine.

### **Summary**

The evaluator confirmed that CAVP testing of all cryptographic operations was performed in accordance with the CAVP test procedures. The results have been validated by the CAVP and the certificate information is provided in section 2.1, "CAVP Summary," in the Assurance Activity Report (AAR).

### **2.3.3.4 Cryptographic Operation (for cryptographic signature) (FCS\_COP.1(2))**

#### **TSS Assurance Activities**

No assurance activities defined.

#### **Guidance Assurance Activities**

No assurance activities defined.

#### **Test Assurance Activities**

#### **Assurance Activity AA-FCS\_COP.1-2-ATE-01**

##### **ECDSA Algorithm Tests**

###### *ECDSA FIPS 186-4 Signature Generation Test*

For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values  $R$  and  $S$ . To determine correctness, the evaluator shall use the signature verification function of a known good implementation.

###### *ECDSA FIPS 186-4 Signature Verification Test*

For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.

##### **RSA Signature Algorithm Tests**

###### *Signature Generation Test*

The evaluator generates or obtains 10 messages for each modulus size/SHA combination supported by the TOE. The TOE generates and returns the corresponding signatures.

The evaluator shall verify the correctness of the TOE's signature using a trusted reference implementation of the signature verification algorithm and the associated public keys to verify the signatures.

###### *Signature Verification Test*

*For each modulus size/hash algorithm selected, the evaluator generates a modulus and three associated key pairs, (d, e). Each private key d is used to sign six pseudorandom messages each of 1024 bits using a trusted reference implementation of the signature generation algorithm. Some of the public keys, e, messages, or signatures are altered so that signature verification should fail. For both the set of original messages and the set of altered messages: the modulus, hash algorithm, public key e values, messages, and signatures are forwarded to the TOE, which then attempts to verify the signatures and returns the verification results.*

*The evaluator verifies that the TOE confirms correct signatures on the original messages and detects the errors introduced in the altered messages.*

## Summary

The evaluator verified the implementation of the digital signature generation and verification methods supported by the TOE using either the Cryptographic Algorithm Validation Program (CAVP), or the applicable tests included in this assurance activity.

### ***RSA Signature Generation PKCS1#v1.5 with SHA2-256, SHA2-384, SHA2-512 for 2048-bit moduli***

*(provided by the Apache NSS cryptographic module for the HTTPS server)*

### ***RSA Signature Verification PKCS1#v1.5 with SHA-1, SHA2-256, SHA2-384, SHA2-512 for 2048, 3072 and 4096-bit moduli***

*(provided by the OpenSSL cryptographic module for the TLS client)*

### ***RSA Signature Verification PKCS1#v1.5 with SHA-1 for 2048, 3072 and 4096-bit moduli***

*(provided by the Bouncy Castle cryptographic module for the SSH client)*

These methods were tested using the CAVP in accordance with the CAVP test procedures. The results have been validated by the CAVP and the certificate information is provided in section 2.1, "CAVP Summary," in the Assurance Activity Report (AAR).

### ***RSA Signature Generation PKCS1#v1.5 with SHA-1 for 2048-bit moduli***

*(provided by the Apache NSS cryptographic module for the HTTPS server)*

The evaluator tested RSA SigGen PKCS#1v1.5 with SHA-1 and 2048-bit RSA keys using a TLS connection between the TOE and a known good implementation of the TLS protocol, forcing the selection of a cipher suite that used RSA signature generation to prove the authenticity of the certificate (e.g. ECDHE\_\*) and also forcing RSA with SHA-1 as the signature algorithm. The evaluator repeated this test at least 10 times and verified that in all cases the TLS handshake was successful and therefore the signature had been verified properly by the TLS peer.

### ***RSA Signature Generation PKCS1#v1.5 with SHA-1 for 2048-bit moduli***

*(provided by the Bouncy Castle cryptographic module for the SSH client)*

The evaluator tested RSA SigGen PKCS#1v1.5 with SHA-1 and 2048-bit RSA keys using a SSH connection between the TOE and a known good implementation of the SSH protocol, enabling public-key user authentication with the 2048-bit RSA key generated by the TOE. The evaluator repeated this test at least 10 times and verified that in all cases that the signatures were sent by the TOE and the SSH peer was able to verify them with the user's RSA public key, therefore authenticate the SSH user.

Notice that all signature generation and verification methods have been also tested implicitly during the execution of the rest of the test suite, especially in the scope of FTP\_ITC.1 and FTP\_TRP.1.

### 2.3.3.5 Cryptographic Operation (for cryptographic hashing) (FCS\_COP.1(3))

#### TSS Assurance Activities

##### Assurance Activity AA-FCS\_COP.1-3-ASE-01

*The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.*

#### Summary

Section 7.1.15 *FCS\_COP.1(3) Cryptographic operation (for cryptographic hashing)* of [ST] describes hash functions. It provides Table 18 "Hash algorithms" outlining, for each cryptographic module, the hash functions, capabilities, and standards used to satisfy the ST claims. The column "Usage" clearly identifies the hash functions associated with other TSF cryptographic functions. For example, the second row lists SHA-1, SHA2-256, SHA2-512 along with their key sizes are used by the SSH client for DH key establishment, RSA signature generation and verification, HMACs, and hash DRBG.

#### Guidance Assurance Activities

##### Assurance Activity AA-FCS\_COP.1-3-AGD-01

*The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.*

#### Summary

Also, section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST.

The evaluator examined section *Security Functionality subsection Cryptographic Support* of the [CCGUIDE] and determined that no user specific configuration exists for all of the cryptographic algorithms and the selection is based on negotiation during SSH/TLS session establishment by the various cryptographic providers (e.g. Apache NSS v3.77, Bouncy Castle v1.68, and OpenSSL v1.0.2p). For example, The syslog-ng client uses OpenSSL for its TLS implementation. OpenSSL is a software module that implements both the TLS protocol and cryptographic algorithms. When communicating with the external audit server (syslog server), the syslog-ng client acts as a TLS client. The syslog-ng client supports TLS 1.2(RFC5246). TLS 1.2, as defined in RFC 5426, can utilize SHA-1, SHA2-256, SHA2-384, SHA2-512. Within the TOE, OpenSSL determines which SHA algorithm to implement without the users input or configuration. This is inline with the various NOTES mentioned above in AA-FCS\_CKM.1-AGD-01.

#### Test Assurance Activities

##### Assurance Activity AA-FCS\_COP.1-3-ATE-01

*The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented testmacs.*



The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

#### Short Messages Test - Bit-oriented Mode

The evaluators devise an input set consisting of  $m+1$  messages, where  $m$  is the block length of the hash algorithm. The length of the messages range sequentially from 0 to  $m$  bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

#### Short Messages Test - Byte-oriented Mode

The evaluators devise an input set consisting of  $m/8+1$  messages, where  $m$  is the block length of the hash algorithm. The length of the messages range sequentially from 0 to  $m/8$  bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

#### Selected Long Messages Test - Bit-oriented Mode

The evaluators devise an input set consisting of  $m$  messages, where  $m$  is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the  $i$ th message is  $m + 99*i$ , where  $1 \leq i \leq m$ . The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

#### Selected Long Messages Test - Byte-oriented Mode

The evaluators devise an input set consisting of  $m/8$  messages, where  $m$  is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the  $i$ th message is  $m + 8*99*i$ , where  $1 \leq i \leq m/8$ . The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

#### Pseudorandomly Generated Messages Test

This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is  $n$  bits long, where  $n$  is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

## Summary

The evaluator confirmed that CAVP testing of all cryptographic operations was performed in accordance with the CAVP test procedures. The results have been validated by the CAVP and the certificate information is provided in section 2.1, "CAVP Summary," in the Assurance Activity Report (AAR).

### 2.3.3.6 Cryptographic Operation (for keyed-hash message authentication) (FCS\_COP.1(4))

#### TSS Assurance Activities

##### Assurance Activity AA-FCS\_COP.1-4-ASE-01

The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

## Summary

Section 7.1.16 FCS\_COP.1(4) Cryptographic operation (for keyed-hash message authentication) of [ST] describes key-hashed functions. It provides Table 19 "Keyed-hash message authentication algorithms" outlining 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].

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_COP.1-4-AGD-01

*The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.*

#### Summary

The evaluator examined section *Server Configurations* subsections *SSH Connections To The Imprivata Appliance* and *SSH Connections From The Imprivata Appliance* of the [CCGUIDE] and determined that no user specific configuration exists for using the values used by the HMAC functions. As stated within the aforementioned [CCGUIDE] section *SSH Connections To The Imprivata Appliance*,

*"The administrator cannot edit or alter this list of MACs. This list is set by default; does not require manual configuration; and rejects all other encryption algorithms"*

## Test Assurance Activities

### Assurance Activity AA-FCS\_COP.1-4-ATE-01

*For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key and message data using a known good implementation.*

#### Summary

The evaluator confirmed that CAVP testing of all cryptographic operations was performed in accordance with the CAVP test procedures. The results have been validated by the CAVP and the certificate information is provided in section 2.1, "CAVP Summary," in the Assurance Activity Report (AAR).

### 2.3.3.7 HTTPS (FCS\_HTTPS\_EXT.1)

## TSS Assurance Activities

### Assurance Activity AA-FCS\_HTTPS\_EXT.1-ASE-01

*The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS\_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality.*

#### Summary

Section 7.1.17 *FCS\_HTTPS\_EXT.1 HTTPS* of [ST] describes HTTPS protocol. It states the following:



- The TOE's Apache HTTP Server handles inbound HTTPS requests, which are from administrative web browsers and agents, by first establishing a TLS connection with the initiating endpoint and then waiting for the endpoint to initiate a request. The HTTPS connection is compliant with [RFC2818].
- The TLS implementation for HTTPS, which uses the Apache NSS cryptographic module, is defined in FCS\_TLS\_EXT.1(S) and described in the TSS section 7.1.21 FCS\_TLS\_EXT.1(S) *HTTPS server*.
- HTTPS uses the following cryptographic functions, which are included in the ST.
  - Asymmetric key generation, verification, and establishment as per FCS\_COP.1(2)
  - 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 uses HTTPS for the Admin Console and Appliance Console via the web browser who act as a client and initiates the connection with the TOE and validates the X.509v3 certificate returned by the TOE via the TLS handshake. The TOE provides assured identification by validating the browser's user via username/password after the TLS connection is established.
- Also, the TOE uses HTTPS to communicate with the agents who initiates the connection with the TOE and validates the X.509v3 certificate returned by the TOE during the TLS handshake. The agent supports assured identification via either the agent's user's username/password or the agent's unique key (i.e., when no user is logged into the endpoint during a Refresh interval). In both cases the TOE validates the authentication credentials after the TLS connection is established.

## Guidance Assurance Activities

No assurance activities defined.

## Test Assurance Activities

### Assurance Activity AA-FCS\_HTTPS\_EXT.1-ATE-01

*Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.*

## Summary

Assurance activities were carried out as part of the FCS\_TLS\_EXT.1 testing.

## 2.3.3.8 Extended: Cryptographic operation (Random Bit Generation) (FCS\_RBG\_EXT.1)

## TSS Assurance Activities

### Assurance Activity AA-FCS\_RBG\_EXT.1-ASE-01

*The evaluator shall examine the TSS to ensure it describes the deterministic random bit generation services provided by either the TSF or the TOE environment, including a description of the entropy source.*

## Summary

Section 7.1.18 *FCS\_RBG\_EXT.1 Cryptographic operation (random bit generation)* of [ST] provides the following description for random number generation services:

- The TOE's cryptographic modules use the /dev/random device as an entropy source which is a software-based noise source. Each DRBG is seeded from this source with a minimum of 256 bits of entropy. /dev/random blocks until its entropy estimator determines that sufficient entropy exists to fulfill the requests.
- Table 20 "DRBG algorithms" lists, for each cryptographic module, the DRBG algorithm, capabilities, and standards used to satisfy the ST claims. This consists of the following:
  - Apache NSS: this module, which is used by the HTTPS server, provides the Hash\_DRBG algorithm with SHA-256 compliant to [SP800-90A-Rev1].
  - Bouncy Castle: this module, which is used by the SSH client, provides the Hash\_DRBG algorithm with SHA-256 compliant to [SP800-90A-Rev1].
  - OpenSSL: this module, which is used by the TLS client, provides the CTR\_DRBG algorithm with AES-256 compliant to [SP800-90A-Rev1].

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_RBG\_EXT.1-AGD-01

*The evaluator shall examine the AGD guidance to ensure it provides clear instructions on how to configure the TOE environment. If any part of the deterministic RBG service is configurable, the evaluator shall ensure that the operational guidance provides clear instructions for how to configure them.*

## Summary

The evaluator examined section *Server Configurations* of the [CCGUIDE] and determined that no user specific configuration exists for the deterministic RBG service.

## Test Assurance Activities

### Assurance Activity AA-FCS\_RBG\_EXT.1-ATE-01

*Documentation shall be produced—and the evaluator shall perform the activities—in accordance with Appendix C.9 Entropy Documentation and Assessment of [ESMPMPV2.1]. This documentation may be included as a supplemental addendum to the Security Target. The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms.*

*The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality.*

*If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 - 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90A).*

If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 - 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

**Entropy input:** the length of the entropy input value must equal the seed length.

**Nonce:** If a nonce is supported (CTR\_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.

**Personalization string:** The length of the personalization string must be  $\leq$  seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is supported, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

**Additional input:** the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

## Summary

The evaluator confirmed that CAVP testing of all cryptographic operations was performed in accordance with the CAVP test procedures. The results have been validated by the CAVP and the certificate information is provided in section 2.1, "CAVP Summary," in the Assurance Activity Report (AAR).

### 2.3.3.9 SSH (FCS\_SSH\_EXT.1)

#### FCS\_SSH\_EXT.1.1

#### TSS Assurance Activities

#### Assurance Activity AA-FCS\_SSH\_EXT.1.1-ASE-01

The evaluator will ensure that the selections indicated in the ST are consistent with selections in the dependent components.

## Summary

For FCS\_SSH\_EXT.1.1, the ST specifies the TOE's SSH implementation complies with RFCs 4251, 4252, 4253, 4254 and 4256, 4344, 6668 as a client.

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] provides the following description:

- The Apache SSHD component of the TOE implements SSHv2 client protocol including SCP, which protects 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 complies with RFCs 4251, 4252, 4253, 4254, 4256, 4344, and 6668.

## Guidance Assurance Activities

No assurance activities defined.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.1-ATE-01

*Note for some Assurance Activities defined in the subsequent FCS\_SSH\_EXT elements, that the exact test configuration will depend on whether the TSF acts as an SSH client (and therefore proposes disallowed algorithms) or as an SSH server (and does not accept certain algorithms). The evaluator is expected to be able to configure the test environment appropriately and perform the testing based on the selection made in FCS\_SSH\_EXT.1.1.*

#### Summary

SSH testing was performed with the use of a script to test all requirements. This script is included with the gathered evidence. The evaluator verified that the SSH connection is initiated by the TOE to the external SCP server for external audit storage in FAU\_STG\_EXT.1 Test 1.

### FCS\_SSH\_EXT.1.2

## TSS Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.2-ASE-01

*The evaluator will check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS\_SSH\_EXT.1.5, and ensure that if password-based authentication methods have been selected in the ST then these are also described.*

#### Summary

For FCS\_SSH\_EXT.1.2, the ST specifies the TOE's SSH implementation supports in accordance to RFC 4252 both public key-based and password-based authentication methods. For FCS\_SSH\_EXT.1.5, the ST selects ssh-rsa as the public key algorithm.

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] provides the following description.

- Apache SSHD supports both public key-based and password-based authentication methods as per [RFC4252].
- (In the evaluated configuration), the TOE supports ssh-rsa (i.e., RSA signatures with PKCS1 1.5 and SHA-1) as the transport public key authentication algorithm and rejects all others.

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.2-AGD-01

*If supported public-key authentication methods are configurable, the evaluator shall verify the guidance documentation includes instructions on configuring these. If the password-based authentication method can be enabled or disabled via configuration setting, the evaluator shall verify this configuration is described in the guidance documentation.*

#### Summary

Section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST.

The evaluator examined section *Server Configurations* subsection *Add SCP Server* of the [CCGUIDE] where there is an information NOTE that states the following:

" NOTE:

*The password authentication method cannot be changed. The SSH Public Key authentication method cannot be changed. The algorithms for the SSH protocol cannot be changed. "*

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.2-ATE-01

- *Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the guidance documentation.*
- *Test 2: [Conditional on selection of 'server' in FCS\_SSH\_EXT.1.1] The evaluator shall choose one public key algorithm supported by the TOE. The evaluator shall generate a new key pair for that algorithm without configuring the TOE to recognize/allow the public key for authentication. The evaluator shall attempt to establish a connection with the new key pair and demonstrate that authentication fails.*
- *Test 3: [Conditional] Using the guidance documentation, the evaluator shall configure the TOE for password-based authentication and demonstrate successful authentication over SSH using a password as an authenticator. The evaluator shall then, re-attempt authentication entering an incorrect password, and demonstrate that the authentication fails.*

## Summary

Test 1 covers successful public key authentication with all supported public key algorithms, and this was tested successfully.

Test 2 was conditional on the selection of server in FCS\_SSH\_EXT.1. This was not selected, so this test was deemed N/A.

Test 3 covers this SSH connection through password-based authentication. Correct and incorrect credentials were used to show the failed connection when using the incorrect password. This was tested successfully.

## FCS\_SSH\_EXT.1.3

### TSS Assurance Activities

#### Assurance Activity AA-FCS\_SSH\_EXT.1.3-ASE-01

*The evaluator shall check that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled.*

## Summary

For FCS\_SSH\_EXT.1.3, the ST specifies the TOE will drop packets greater than 32K bytes in an SSH transport connection in accordance to RFC 4253.

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] provides the following description.

- 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).

### Guidance Assurance Activities

No assurance activities defined.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.3-ATE-01

*The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.*

## Summary

The packet size test is performed with the purpose of verifying that the TOE drops a packet received from the external SSH server when it is greater than 32K bytes. The evaluator confirmed that the packet was dropped and the connection was closed by the TOE.

## FCS\_SSH\_EXT.1.4

### TSS Assurance Activities

#### Assurance Activity AA-FCS\_SSH\_EXT.1.4-ASE-01

*The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.*

## Summary

For FCS\_SSH\_EXT.1.4, the ST specifies the following encryption algorithms used for the SSH transport implementation:

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

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] states that the TOE supports the following PP-specified encryption algorithms and rejects all others.

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

The above algorithms are consistent with those specified in FCS\_COP.1(1).

The TSS does not specify any optional characteristics supported by the TOE.

### Guidance Assurance Activities

#### Assurance Activity AA-FCS\_SSH\_EXT.1.4-AGD-01

*The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).*

## Summary

Section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST. This is in line with the following guidance the evaluator found from the [CCGUIDE]:

Section *SSH Connections From The Imprivata Appliance* indicates that the SSH protocol is implemented using Bouncy Castle v1.68 provided through Apache MINA which uses default MAC configuration. The administrator cannot edit or alter this list of MACs.

Section *Configure SCP for Audit Records* contains the following note stating that the SSH public key is set by default, does not require manual configuration and the TOE rejects all other algorithms.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.4-ATE-01

- *Test 1: The evaluator shall establish an SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.*
- *Test 2: The evaluator shall run a test such that only the 3des-cbc encryption algorithm is configured and no other encryption algorithms. The evaluator shall attempt to establish an SSH connection and observe that the connection is rejected.*

## Summary

Test 1 was performed with the intent of verifying successful handshakes using the claimed encryption algorithms listed in the [ST]. These tests were successful.

Test 2 was then performed to verify that an unclaimed and unsupported encryption algorithm of 3des-cbc resulted in a failed SSH connection and a failure log on the TOE.

### FCS\_SSH\_EXT.1.5

## TSS Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.5-ASE-01

*The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms specified are identical to those listed for this component.*

## Summary

For FCS\_SSH\_EXT.1.5, the ST selects ssh-rsa as the public key algorithm used for the SSH transport implementation.

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] states that the TOE supports the following PP-specified transport public key authentication algorithm and rejects all others.

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

The above algorithm is consistent with that specified in FCS\_COP.1(2).

The TSS does not specify any optional characteristics supported by the TOE.

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.5-AGD-01

*The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).*



## Summary

Section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST. This is in line with the following guidance the evaluator found from the [CCGUIDE]:

Section *SSH Connections From The Imprivata Appliance* indicates that the SSH protocol is implemented using Bouncy Castle v1.68 provided through Apache MINA which uses default MAC configuration. The administrator cannot edit or alter this list of MACs.

Section *Configure SCP for Audit Records* contains the following note stating that the SSH public key is set by default, does not require manual configuration and the TOE rejects all other algorithms.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.5-ATE-01

- *Test 1: The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.*
- *Test 2: The evaluator shall attempt to establish an SSH connection where only the ssh-dsa public key algorithm is configured and no other public key algorithms, and observe that the connection is rejected.*

## Summary

Test 1 was performed to verify successful handshakes with the selected public key algorithms listed in the [ST]. These tests were successful.

Test 2 was then performed to verify handshake failure using the invalid public key authentication method of ssh-dsa.

## FCS\_SSH\_EXT.1.6

### TSS Assurance Activities

#### Assurance Activity AA-FCS\_SSH\_EXT.1.6-ASE-01

*The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that that list corresponds to the list in this component.*

## Summary

For FCS\_SSH\_EXT.1.6, the ST specifies the following as the data integrity algorithms used for the SSH transport implementation:

- hmac-sha1
- hmac-sha1-96
- hmac-sha2-256
- hmac-sha2-512

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] states that the TOE supports the following PP-specified data integrity algorithms and rejects all others.

- hmac-sha1
- hmac-sha1-96
- hmac-sha2-256



- hmac-sha2-512

The above algorithms are consistent with those specified in FCS\_COP.1(4).

The TSS does not specify any optional characteristics supported by the TOE.

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.6-AGD-01

*The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).*

#### Summary

Section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST. This is in line with the following guidance the evaluator found from the [CCGUIDE][a](#):

Section *SSH Connections From The Imprivata Appliance* indicates that the SSH protocol is implemented using Bouncy Castle v1.68 provided through Apache MINA which uses default MAC configuration. The administrator cannot edit or alter this list of MACs.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.6-ATE-01

- *Test 1: The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.*
- *Test 2: The evaluator shall attempt to establish an SSH connection, using the TSF, where only the "none" MAC algorithm is configured, and observe that the attempt fails.*
- *Test 3: The evaluator shall attempt to establish an SSH connection, using the TSF, where only the hmac-md5 MAC algorithm is configured and observe that the attempt fails.*

#### Summary

Test 1 covers the claimed integrity algorithms listed in the [ST][a](#). All claimed algorithms were tested successfully.

Test 2 covered using the MAC specification of "none" to verify that the connection was unsuccessful. This successfully failed, and failure logs were captured by the TOE.

Test 3 covered the unclaimed and unsupported integrity algorithm of hmac-md5 to verify that the connection was unsuccessful. This successfully failed and generated a failure log on the TOE.

## FCS\_SSH\_EXT.1.7

## TSS Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.7-ASE-01

*The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that that list corresponds to the list in this component.*

## Summary

For FCS\_SSH\_EXT.1.7, the ST selects diffie-hellman-group14-sha1 as the key exchange method used for the SSH transport implementation.

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] states that the TOE supports the following key exchange/establishment method and rejects all others.

- diffie-hellman-group14-sha1

The above algorithm is consistent with that specified in FCS\_CKM.1.

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.7-AGD-01

*If key exchange methods are configurable, the evaluator shall check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections to the TOE.*

## Summary

Section *Install Common Criteria Feature Flag* describes the IPM patch which enables the TOE functionality inclusive to the evaluated configuration including restricting the SSH algorithms as well as TLS versions and ciphersuites to those claimed in the ST. This is in line with the following guidance the evaluator found from the [CCGUIDE]:

Section *SSH Connections From The Imprivata Appliance* indicates that the SSH protocol is implemented using Bouncy Castle v1.68 provided through Apache MINA which uses default MAC configuration. The administrator cannot edit or alter this list of MACs.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.7-ATE-01

- *Test 1: The evaluator shall configure an SSH connection to permit all allowed key exchange methods. The evaluator will attempt to establish an SSH connection with the TOE using each allowed key exchange method and observe that each attempt succeeds.*
- *Test 2: The evaluator shall attempt to establish an SSH connection, using the TSF, where the SSH client only allows the diffiehellman-group1-sha1 key exchange and the SSH server is configured according to the algorithms allowed in the SFR. The evaluator shall observe that the attempt fails.*

## Summary

Test 1 covers the claimed key exchange methods listed in the [ST]. These methods were tested successfully.

Test 2 covered the unsupported kex algorithm of diffie-hellman-group1-sha1 to verify that the connection was unsuccessful. This connection failed, and a failure log was captured on the TOE.

## FCS\_SSH\_EXT.1.8

## TSS Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.8-ASE-01

*The evaluator shall check the TSS to ensure that if the TOE enforces connection rekey or termination limits lower than the maximum values that these lower limits are identified.*

*In cases where hardware limitation will prevent reaching data transfer threshold in less than one hour, the evaluator shall check the TSS to ensure it contains:*

- a. *An argument describing this hardware-based limitation and*
- b. *Identification of the hardware components that form the basis of such argument. For example, if specific Ethernet Controller or Wi-Fi radio chip is the root cause of such limitation, these subsystems shall be identified.*

## Summary

For FCS\_SSH\_EXT.1.8, the ST specifies the following conditions for a connection to rekey:

- no more than 1 Gigabyte of data has been transmitted using that key

Section 7.1.19 *FCS\_SSH\_EXT.1 SSH* of [ST] states that the TOE will rekey a connection after the following conditions:

- no more than 1 Gigabyte of data has been transmitted

The TSS does not specify any hardware-based limitation that would prevent reaching data transfer threshold in less than one hour; therefore, no description is necessary.

## Guidance Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.8-AGD-01

*The evaluator shall check the guidance documentation to ensure that if the connection rekey or termination limits are configurable, it contains instructions to the administrator on how to configure the relevant connection rekey or termination limits for the TOE.*

## Summary

[CCGUIDE] section "SSH Connections From The Imprivata Appliance" contains the following statement:

*" Imprivata OneSign will automatically rekey the SSH connection after the conditions stated in the Security Target. "*

Thus, the evaluator determined no guidance is necessary.

## Test Assurance Activities

### Assurance Activity AA-FCS\_SSH\_EXT.1.8-ATE-01

*The test harness needs to be configured so that its connection rekey or termination limits are greater than the limits supported by the TOE -- it is expected that the test harness should not be initiating the connection rekey or termination.*

- *Test 1. Establish an SSH connection. Wait until the identified connection rekey limit is met. Observed that a connection rekey or termination is initiated. This may require traffic to periodically be sent, or connection keep alive to be set, to ensure that the connection is not closed due to an idle timeout.*

## Summary

The final SSH test involves the TOE initiating a rekey after roughly 1 GB of data has been sent across the connection. The evaluator setup the SSH connection from the TOE to the external audit server and verified that the rekey was successful and initiated by the TOE. After the rekey, data continued to be protected via the SSH protocol.

### 2.3.3.10 TLS (FCS\_TLS\_EXT.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FCS\_TLS\_EXT.1-ASE-01

*The evaluator shall check the TSS to ensure that it describes whether the TOE acts as a TLS server, TLS client, or both and map this to specific trusted path/channel cases. If a specific TLS application is not part of the evaluated configuration, the TSS shall identify it, specifically declare it as out of scope, and declare whether it is disabled by default.*

*The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified include those listed for this component.*

#### Summary

The ST defines the following iterations of FCS\_TLS\_EXT.1

- FCS\_TLS\_EXT.1(C) TLS client (syslog-ng)
- FCS\_TLS\_EXT.1(S) HTTPS server

Thus, in the evaluated configuration, the TOE acts as both a TLS client and a TLS server.

Section 7.1.20 *FCS\_TLS\_EXT.1(C) TLS client (syslog-ng)* of [ST] describes the TOE acting as a TLS client (i.e., syslog-ng client) when communicating with the external audit server (syslog server). It supports TLS 1.2 with the following PP-specified 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

Section 7.1.21 *FCS\_TLS\_EXT.1(S) HTTPS server* of [ST] describes the TOE acting as a TLS server (i.e., Apache HTTP Server) to handle inbound HTTPS requests. It supports TLS 1.2 with the following PP-specified 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
- 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

#### Guidance Assurance Activities

##### Assurance Activity AA-FCS\_TLS\_EXT.1-AGD-01

*The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the product so that TLS conforms to the description in the TSS. If administrative steps need to be taken to disable a specific TLS application or so that the cipher suites negotiated by the implementation are limited to those in this requirement, then the appropriate instructions need to be contained in the guidance.*

## Summary

[CCGUIDE] section *Cryptographic Support* states that the syslog-ng client supports TLS 1.2 (RFC5246) for communicating with the external audit server (syslog). It rejects all other TLS versions. It uses the OpenSSL v1.0.2p software library (module) for its TLS implementation and cryptographic provider. It also states that the syslog-ng client supports the following 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

Also in the same section, the [CCGUIDE] states that the TOE's Apache HTTP Server, acts as an HTTPS server handling inbound HTTPS requests. The Apache HTTP Server supports TLS 1.2 (RFC5246) 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 (module) for its TLS implementation and cryptographic provider. It supports the following 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
- 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

The [CCGUIDE] section *Trusted Path/Channels* states the following concerning the trusted communications:

- The TOE acts as an HTTPS server supporting TLS 1.2 when communicating with the agents.
- The TOE uses TLS 1.2 to protect the communication channel when transferring audit data from the TOE to the external audit server (syslog).

Section *Remote Syslog Server* contains the following note:

*" NOTE: TLS, Bouncy Castle, and NSS are the only cryptography engines used by Imprivata OneSign. Imprivata OneSign administrators cannot configure this. Any other cryptography engines are prohibited in the Common Criteria evaluated configuration. "*

For this statement, the evaluator concluded that these are the only cryptographic service providers supported in the evaluated configuration by default. As pointed out in other work units, the administrator is required to install the "CC mode" flag described in section *Install Common Criteria Feature Flag* which restricts these TLS providers (Apache NSS and OpenSSL) to support only the

TLS versions and ciphersuites claimed in the ST. The additional step the administrator has to perform is to enable TLS support for the remote syslog server as instructed in this same section *Remote Syslog Server*.

## Test Assurance Activities

### Assurance Activity AA-FCS\_TLS\_EXT.1-ATE-01

The evaluator shall also perform the following tests for each use of TLS in the TOE (as defined in the TSS):

- **Test 1:** The evaluator shall establish a TLS connection using each claimed cipher suite specified by the requirement. It is sufficient to observe the successful handshake following the negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
- **Test 2:** The evaluator shall perform the following modifications to the Client/Server Hellos:
  - **Test 2a:** [conditional on TOE implementing TLS client] The evaluator shall send a Server Hello containing only the TLS\_NULL\_WITH\_NULL\_NULL cipher suite and verify that the TOE denies the connection.
  - **Test 2b:** [conditional on TOE implementing TLS Server] The evaluator shall send a Client Hello containing only the TLS\_NULL\_WITH\_NULL\_NULL cipher suite and verify that the TOE denies the connection.
- **Test 3:** The evaluator shall perform the following modifications to the traffic:
  - **Test 3a:** [conditional on TOE implementing TLS client]
    - **Test 3a.1:** Change the TLS version sent in the Server Hello to an undefined TLS version (for example 1.5 represented by the two bytes 03 06) and verify that the TOE rejects the connection.
    - **Test 3a.2:** Change the TLS version sent in the Server Hello to the most recent unsupported TLS version (for example 1.1 represented by the two bytes 03 02) and verify that the TOE rejects the connection.
    - **Test 3a.3:** If DHE or ECDHE cipher suites are supported, modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the handshake is not completed and no application data flows. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
    - **Test 3a.4:** [conditional] If DHE or ECDHE cipher suites are supported, modify the signature block in the server's Key Exchange handshake message, and verify that the handshake does not complete and no application data flows. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
    - **Test 3a.5:**
      - **Test 3a.5a:** Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator shall verify that the client does not complete the handshake and no application data flows.
      - **Test 3a.5b:** Modify a byte in the Server Finished handshake message and verify the client does not complete the handshake and no application data flows.
      - **Test 3a.5c:** Send a garbled message from the server after the server has issued the Change Cipher Spec message and verify that the client does not complete the handshake and no application data flows. The garbled message must still have a valid 5-byte (1 byte record type, followed by 2 byte version, and 2 byte length) record layer header with matching version in order to ensure the message will be parsed appropriately. For example, for TLS v1.2 Change Cipher Spec (14 03 03 00 01 01) followed by a garbled message (16 03 03 00 40 14 00 00 ...).
  - **Test 3b:** [conditional on TOE implementing TLS server]
    - **Test 3b.1:** Change the TLS version sent in the Client Hello to the most recent unsupported TLS version (for example 1.1 represented by the two bytes 03 02) and verify that the TOE rejects the connection.
    - **Test 3b.2:**
      - **Test 3b.2a:** Modify a byte in the data of the client's Finished handshake message and verify the server rejects the connection and does not send any application data.
      - **Test 3b.2b:** Demonstrate that the TOE will not resume a session for which the client failed to complete the handshake (independent of TOE support for session resumption). Generate a Fatal Alert by sending a Finished message from the client before the client sends a ChangeCipherSpec message, and then send a ClientHello with the session identifier from the previous incomplete session and verify the server does not resume the session.



- **Test 3b.2c:** Send a garbled message from the client after the client has issued the Change Cipher Spec message and verify that the server does not complete the handshake and no application data flows. The garbled message must still have a valid 5-byte (1 byte record type, followed by 2 byte version, and 2 byte length) record layer header with matching version in order to ensure the message will be parsed appropriately. For example, for TLS v1.2 Change Cipher Spec (14 03 03 00 01 01) followed by a garbled message (16 03 03 00 40 14 00 00 ...).

&gt;

## Summary

Test 1: TLS testing was implemented with the TOE serving as both a TLS client and server. All claimed ciphersuites from the [ST] were successfully tested for both implementations.

Test 2a: The TOE was implemented as a TLS client for this test case. A Server Hello message containing the TLS\_NULL\_WITH\_NULL\_NULL ciphersuite is sent to the TOE from our syslog server, and the evaluator verified that the TOE correctly denied the connection based on this incorrect ciphersuite.

Test 2b: The TOE was implemented as a TLS server for this case. A Client Hello message containing the TLS\_NULL\_WITH\_NULL\_NULL ciphersuite is sent to the TOE, and the evaluator verified that the TOE correctly denied the connection based on this incorrect ciphersuite.

Test 3a.1: The TOE was implemented as a TLS client for these sub-test cases. A Server Hello message was sent using an undefined TLS version. Packet captures in evidence show the TLS version as "Unknown (0x0306)" and the TOE correctly denies this connection.

Test 3a.2: The TLS version in the Server Hello message was changed to verify that invalid protocols were not accepted by the TOE. These invalid protocols included SSL2.0, SSL3.0, TLS1.0, and TLS1.1. All connections were correctly denied by the TOE.

Test 3a.3: A modification was made to the server's nonce in the Server Hello message. The first byte of the nonce was altered, and the TOE correctly denied this connection after this modification.

Test 3a.4: A modification was made to the signature block in the Server's KeyExchange handshake message. This was achieved with a valid RSA certificate on our test server with the option "ModifySignatureBlockInKeyExchange". The TOE successfully denied this connection.

Test 3a.5a: This test case involved the modification of the selected ciphersuite in the Server Hello message not present in the Client Hello message. The TOE correctly denied this connection.

Test 3a.5b: A modification was made to the first byte in the ServerFinished handshake message. This was tested to verify the client does not complete the handshake and that no application data flows. The TOE successfully denied this connection.

Test 3a.5c: This test case involved sending a garbled message after the ChangeCipherSpec message from the test server. The TOE successfully denied this connection.

Test 3b.1: The TOE was implemented as a TLS server for these sub-test cases. The evaluator verified that the TOE denied connections that were attempted with the invalid protocols SSL2.0, SSL3.0, TLS1.0, TLS1.1, and TLS1.3.

Test 3b.2a: A modification was made in the Client Finished handshake message that changed the first byte. The TOE correctly denied this connection.

Test 3b.2b: This test was achieved by attempting to send a Client Hello message with the same session identifier used in a previous fatal alert. The TOE correctly denied this connection.

Test 3b.2c: This last test case involved sending a garbled message after issuing the ChangeCipherSpec message. The TOE correctly denied this connection.

## 2.3.4 Identification and authentication (FIA)

### 2.3.4.1 Authentication failure handling (FIA\_AFL.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FIA\_AFL.1-ASE-01

*The evaluator shall check the TSS in order to determine that the authentication failure handling function is described in sufficient detail to affirm the SFR.*

#### Summary

Section 7.1.22 FIA\_AFL.1 Authentication failure handling of [ST] states the following:

- 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.

#### Guidance Assurance Activities

##### Assurance Activity AA-FIA\_AFL.1-AGD-01

*The evaluator shall check the operational guidance to verify that a discussion on authentication failure handling is present and consistent with the representation in the Security Target.*

#### Summary

The [CCGUIDE] section Security Functionality subsection Identification and Authentication states that the TOE enforces authentication failure handling for both Admin and Appliance Consoles with more guidance specified in the User Lockout Policy, which is a component of the User Policy. The [CCGUIDE] section User Lockout Policy provides a detailed description of what the lockout policy is and how the administrator configures both the number of consecutive authentication attempts and the period of time of the unsuccessful attempts to occur within. The section provides step-by-step instructions on how to configure the lockout rules. Within the instructions, the [CCGUIDE] specifies the default number of consecutive failures (at 5) and the default amount of time an account is locked (5 minutes).

#### Test Assurance Activities

##### Assurance Activity AA-FIA\_AFL.1-ATE-01

*The evaluator shall test this capability by using the authentication function of the TSF to deliberately enter incorrect credentials. The evaluator shall observe that the proper action occurs after a sufficient number of incorrect authentication attempts. The evaluator shall also use the TSF to reconfigure the threshold value in a manner consistent with operational guidance to verify that it can be changed.*

#### Summary

Incorrect credentials were deliberately entered into the Appliance Console, Admin Console, and Agent installed on the evaluator's endpoint. This was for the purpose of verifying that the TOE acted in accordance with its login failure settings on each TSFI. The evaluator set the user accounts to lockout after 3 failed login attempts for 5 minutes. It was confirmed that the TOE locked out the user account for the full duration of the 5-minute period, and recorded the required logs.



## 2.3.4.2 User-Subject Binding (FIA\_USB.1)

### TSS Assurance Activities

#### Assurance Activity AA-FIA\_USB.1-ASE-01

*The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them.*

#### Summary

Section 7.1.23 *FIA\_USB.1 User-subject binding* of [ST] provides the following description:

- Each administrator has one or more roles (security attribute) assigned to their account in the TOE's database.
- Upon successful login, the administrator role attributes of each role assigned to the administrator are combined to provide full access rights.
- Any changes to the role attributes assigned to a role before session login or during active session do not take effect until the next login.
- Roles are assigned to administrators as specified in Table 10 "Management functions" (entry FMT\_SMF.1) in the TSS. Section 7.1.28 *FMT\_SMR.1 Security Roles* further discusses the supported roles. The evaluator examined Table 10 along with section 7.1.28 and determined that it describes the different administrative roles supported by the TOE in the evaluated configuration.

### Guidance Assurance Activities

#### Assurance Activity AA-FIA\_USB.1-AGD-01

*The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.*

#### Summary

[CCGUIDE] Chapter *Administrator Roles (Delegated Administration)* describes the roles for Administrators. It should be noted that within this section, Delegated Administrator is referenced as administrator. The evaluator found this acceptable since Super Administrator is always referenced as Super Administrator, and thus, there is no confusion between the two. Also, the [CCGUIDE] states the following in the *Administrator Roles (Delegated Administration)* section:

*" Imprivata uses administrator roles and sub-Administrator roles with nested scope so you can delegate administrative authority throughout the enterprise. "*

Section *The Super Administrator* states that there is only one Super Administrator role and it cannot be edited or deleted. The Super Administrator can perform all the operations of the enterprise. All other administrator roles are subordinate to the Super Administrator role. Section *Administrators* states that

*"Administrators in subordinate roles can run reports allowed by their role, but they do not see results from actions that occur outside their scope."*

The [CCGUIDE], section *Administrator Operations*, provides four tables that list the attributes that are available and can be assigned to administrator roles in the evaluated configuration. The attributes relevant are restated in the tables below:

**Table 3: Administrator Role Attributes**

Operations(s)	Description
<b>Properties</b>	
Update System Properties	Ability to define system operations and maintenance including setting refresh interval.
System Lockdown	Administrators with System Lockdown privileges can still access Imprivata applications when they are locked down.
Maintain Audit Log	Gives the user the ability to maintain Imprivata audit logs. Users with this role are allowed to either delete and archive, only archive or only delete audit records.
Download Agent MSI Files	Allows the user to download the agent MSI files.
Create/Edit Security Questions Delete Security Questions	Allows users to maintain security questions that are used by Imprivata OneSign Self-Services.
<b>Policies</b>	
Create/Edit User Policy Delete User Policy Assign User Policy	User policy are assigned to users across the enterprise. User policies apply to the user wherever the user authenticates User policies allow you to set different authentication parameters for different user groups.
Update Computer Policy Delete Computer Policy	Computer policies govern security-related behaviors that are controlled at specific computers.
<b>Users</b>	
Add/Edit Users	Allows the administrator to add or edit users
Enable/Disable User	Allows the administrator to enable and disable users.
Delete User	Allows the administrator to delete users from the Imprivata directory.
Reset Imprivata Directory User Password	Allows the administrator to reset an Imprivata user's password.
Trust/Upload TLS Certificate Delete TLS Certificate	Allows the administrator to upload new TLS certificates or delete an existing trusted TLS certificate.
Update Computers Delete Computers Assign Computer Policy	Allows the administrator to assign computer policies.
Create/Edit Administrator Roles Delete Administrator Roles	Allows the administrator to create and delete additional administrator roles. There can only be one Super Administrator role.
<b>Reports</b>	
View Report Update Report	Allows the administrator to view and update Imprivata reports.
Delete Report	Allows the administrator to delete existing Imprivata reports.
Export Report	Allows the administrator to export Imprivata data to a .CSV file.

## Test Assurance Activities

### Assurance Activity AA-FIA\_USB.1-ATE-01

*The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.*

### Summary

NOTE that the TOE does not support external sources to store information. As described in section 1.5 of the [ST], the TOE includes "Oracle Database 19 - used to store user accounts, user authentication data, policies, and audit data.". Therefore, the test cases designed for verifying his SFR do not include steps for configuring or using external sources. The test cases are designed to demonstrate that authentication and access control policies enforced by the TOE are consistent with the user information input through the use of the Security Management functions provided by the TOE.

Test 1 is to verify that role types can be created with attributes and a TSF access control policy. The TSF is setup to accept user information from the TOE's internal database during the initial TOE setup process prior to testing. Three new users were created: one admin user, one non-admin user, and one delegated admin user with a custom role for the purpose of this test.

The evaluator verified that the roles were assigned successfully and were reflected by the TOE. The roles were chosen with the purpose of showing all possibilities, with the non-admin user showing no access, the delegated admin user showing access with limited functionality, and the admin user showing full access.

Test 2 is to verify the functionality for the user roles, and to observe that the user authorizations are consistent with their defined attributes and the configuration of the TSF's access control policy.

The normal user's functionality was observed, followed by updating that user to an administrator. After the update, admin functionalities were verified and no non-admin functionalities were lost. The delegated admin user's functionality was observed by attempting to disable a user once authenticated on the TOE. Testing showed that the limitations placed on the custom delegated role were reflected accurately by the TOE. After updating the custom delegated role, changes were then allowed to be made.

For Test 3, the evaluator verified that any changes to role and role assignments did not take effect until the user in question logs out and back into the TOE. Functionality was not updated until the next login, as expected.

## 2.3.5 Security management (FMT)

### 2.3.5.1 Management of functions behaviour (FMT\_MOF.1)

## TSS Assurance Activities

### Assurance Activity AA-FMT\_MOF.1-ASE-01

*The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.*

## Summary

According to the Application Note, the first assignment in FMT\_MOF.1 is expected to correspond with the management functions that are defined in FMT\_SMF.1.

Section 7.1.24 *FMT\_MOF.1 Management of security functions behavior* of [ST] states that the information for this TSS has been included in the TSS for FMT\_SMF.1; thus, the evaluator performed this assurance activity in conjunction with FMT\_SMF.1 where the evaluator verified that both SFR's define the same set of management functions. In addition, the TSS for FMT\_SMF.1 provides Table 21 "Security management functions" lists the management functions and authorizations (i.e., admin roles/role attributes) that can perform these functions.

## Guidance Assurance Activities

### Assurance Activity AA-FMT\_MOF.1-AGD-01

*The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this.*

## Summary

The [CCGUIDE] section *Administrator Roles (Delegated Administration)* states that the TOE's Admin Console supports the two types of administrator roles that are also defined in the [ST] as Super Administrator and Delegated Administrator. The [CCGUIDE] states that 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. Delegated Administrators roles are assigned unique names.

Section *Administrator Roles (Delegated Administration)* further explains the administrator levels/roles. It that delegated administration employs three important concepts: administrative operations, scope of delegation, and inheritance of these two properties. Section *Administrator Levels* states that there can be any number of users assigned to an administrator role and that all administrator roles are created from the Super Administrator role.

Section *The Super Administrator* indicates that there is only one Super Administrator role and it cannot be edited or deleted. The Super Administrator can perform all operations in the enterprise, and all other administrator roles are subordinate to the Super Administrator role. The following section *Administrators* explains that the Super Administrator can create as many subordinate roles as it needs and can have any number of users in each role. Each administrator is a member of an administrator role. Multiple Administrators can share a role, but an administrator can have only one administrator role.

Section *Administrator Operations* explains that the TOE provides a fine granularity of operations that a delegated administrator can perform and provides tables *Administrator Role Attributes* that list the attributes that are available and can be assigned to administrator roles. Within section *Administrator Roles (Delegated Administration)* subsection *The Super Administrator*, it is indicated that the Admin Console Super Administrator can perform all appliance administration functions across the enterprise; while in section *Administrators* it is stated that an Administrator (i.e. a delegated administrator) cannot perform some actions that affect the entire enterprise.

## Test Assurance Activities

### Assurance Activity AA-FMT\_MOF.1-ATE-01

*The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.*

#### Summary

NOTE The TSF cannot be configured externally by any management product, and all functions of the TSF are limited to administrative accounts.

All management functions listed in [ST] Table 10 were tested, and logs for each function were successfully recorded. The evaluator was able to record example logs for each administrative function and reference where in the [DTR] these logs were collected from.

Access to the TOE TSFIs are only available to administrators, as shown in ESM\_EAU.2 Test 1 and FIA\_USB.1 Tests 1 and 3. The evaluator was able to confirm that unprivileged accounts were not able to access the management interfaces needed to perform management functions. Without having the role of an administrator, a user has no ability to perform management functions.

### 2.3.5.2 External Management of Functions Behavior (FMT\_MOF\_EXT.1)

## TSS Assurance Activities

### Assurance Activity AA-FMT\_MOF\_EXT.1-ASE-01

*The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it summarizes the Access Control product functions that the TOE is able to manage and the authorizations that are required in order to manage these functions.*

#### Summary

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

Section 7.1.25 FMT\_MOF\_EXT.1 External management of functions behavior of [ST] provides the following description covering the required management functions for the agent (Access Control product) and the necessary authorizations to perform these functions:

- Audited events: query and modify the set of rules for excluding audited events from a master set of events of all agents. The administrator must have the *Update System Properties* role attribute
- Repository for trusted audit storage: query and modify the agent's repository location for the audit log storage. The administrator must have the *Maintain Audit Log* role attribute.
- Access control SFP: query and modify Computer Policy and User Policy. The administrator must have the *Create/Edit Computer Policy* and *Create/Edit User Policy* role attribute.

- Policy being implemented by the TSF: query the User Policy and Computer Policy and modify (apply) a different policy. The administrator must have the *Assign User Policy* and *Assign Computer Policy* role attribute.
- Access control SFP behavior to enforce in the event of communications outage: query and modify the agent's Offline Authentication mode. The administrator must have the *Create/Edit User Policy* role attribute.
- Refresh interval: query and modify the global Refresh Internal value. The administrator must have the *Update System Properties* role attribute.

## Guidance Assurance Activities

### Assurance Activity AA-FMT\_MOF\_EXT.1-AGD-01

The evaluator shall check the operational guidance in order to determine that it provides instructions for how to connect to an Access Control product and what privileges are required to perform management functions on it once the connection has been established.

### Summary

The [ST] section 7.1.25 *FMT\_MOF\_EXT.1 External management of functions behavior* lists the Access Control product functions of the agent. The [ST] also notes that the TOE never contacts the agent, the agent contacts the TOE under the conditions described in section 1.5.2.1.5 *Security management*. The evaluator decided to take the list of Access Control product functions listed in the [ST] and create the following table mapping the [CCGUIDE] reference to the function:

**Table 4: Access Control Functions**

Management functions	Operations	Role Attribute
Audited events	A TOE administrator 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.	<b>Update System Properties</b> administrator role attribute [CCGUIDE], section <i>Administrator Operations</i> , table <i>Properties</i>
Repository for trusted audit storage	A TOE administrator can query and modify the agent's repository location for the audit log storage via the Admin Console.	<b>Maintain Audit Log</b> administrator role attribute [CCGUIDE], section <i>Administrator Operations</i> , table <i>Properties</i>
Access control SFP	A TOE administrator can query and modify the User and Computer Policy currently enforced by the agent via the Admin Console.	<b>Create/Edit User Policy</b> administrator role attribute [CCGUIDE], section <i>Administrator Operations</i> , table <i>Policies</i> <b>Create/Edit Computer Policy</b> administrator role attribute [CCGUIDE], section <i>Administrator Operations</i> , table <i>Policies</i>
Policy being implemented by the TSF	A TOE administrator 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.	<b>Assign User Policy</b> [CCGUIDE], section <i>Administrator Operations</i> , table <i>Policies</i> and <b>Assign Computer Policy</b> administrator role attributes [CCGUIDE], section <i>Administrator Operations</i> , table <i>Users</i>



Management functions	Operations	Role Attribute
Access control SFP behavior to enforce in the event of communications outage	A TOE administrator can query and modify the agent's Offline Authentication mode via the Admin Console. <sup>1</sup>	<b>Create/Edit User Policy</b> administrator role attribute [CCGUIDE] <a href="#">📄</a> , section <i>Administrator Operations</i> , table <i>Policies</i>
Refresh Interval	An administrator on the TOE can query and modify the global Refresh Interval value under the Settings menu of the Admin Console.	<b>Update System Properties</b> [CCGUIDE] <a href="#">📄</a> , section <i>Administrator Operations</i> , table <i>Policies</i>

The evaluator verified that each of the role attributes defined in table **Access Control Functions** are also defined in the [CCGUIDE] [📄](#). Subsection *Administrator Operations*, which contains various tables within the *Properties* subsection, lists the operations that are available and can be assigned to different administrator roles. Once assigned, the administrators then have the ability to affect the agent utilizing the various operations via their respective Admin Consoles. These operations are:

- Update System Properties
- Maintain Audit Log
- Create/Edit User Policy
- Assign User Policy
- Assign Computer Policy
- Update Computer Policy

Any updates made to the User or Computer Policies that would affect the agent by the administrator are pushed to their respective endpoints upon their refresh interval. This is outlined in section *Computers and Computer Policy* of the [CCGUIDE] [📄](#) which states:

*" Changes to computer policy are sent to Imprivata agents at affected computers at the next refresh interval. "*

This is also touched upon in section *Users and User Policy* of the [CCGUIDE] [📄](#) which states:

*"Changes to user policy are sent to Imprivata agents at the next refresh interval."*

## Test Assurance Activities

### Assurance Activity AA-FMT\_MOF\_EXT.1-ATE-01

*The evaluator shall test this capability by deploying the TOE in an environment where there is an Access Control component that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.*

<sup>1</sup> Per the [ST] [📄](#) section 7.1.25 FMT\_MOF\_EXT.1 External management of functions behavior:

*" 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, 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. "*



The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:

- *Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior*
- *Repository for audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository*
- *Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP.*
- *Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.*
- *Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.*

Once this has been done, the evaluator shall reconfigure the TOE so that it is no longer authorized to manage the Access Control product. The evaluator shall then attempt to perform management functions using the TOE and observe that this is either disallowed or that the option is not even present.

## Summary

NOTE that many of the management functions required here have already been tested. Testing on policy enforcement and modifications can be found in ESM\_ACD.1 Test 1, ESM\_ACT.1 Test 1, and ESM\_ACD.2 Test 1. The TOE has demonstrated the ability to accurately manage computers and users based off these policies, and modifications to these policies were applied appropriately on the agent.

Below is a summary of where each management function has been previously tested:

- Audited Events – this management function was tested in FAU\_SEL\_EXT.1 Test 1.
- Repository for audit storage – this management function was tested in FAU\_STG\_EXT.1 Test 1.
- Access Control SFP – this management function was tested in ESM\_ACT.1 Test 1.
- Policy being implemented by the TSF – this management function was tested in ESM\_ACD.1 Test 1.
- Access control SFP behavior in the event of an outage – this management function was tested in FTP\_ITC.1 Test 4 for the agent.
- Refresh Interval – this management function was tested in ESM\_ACT.1 Test 1.

Test 1 is performed with the purpose of issuing the administrative modifications list in [ST] [\[ST\]](#). The evaluator only tested management functions that are not listed in the NOTE above as already tested. The modifications were made within the Default Computer Policy for this test. A local log repository for the agent was enabled, and the evaluator verified that events were successfully recorded. The refresh interval function was also shown during this test, but specific testing for the refresh interval can be found in ESM\_ACT.1 Test 1.

The modifications were made within the Default Computer Policy for this test. After testing these functions, the evaluator removed the Access Control device from the TOE and attempted to manage the device. This was shown to not be possible.

All functions of the TSFIs are limited to administrative accounts, as shown in ESM\_EAU.2 Test 1 and FIA\_USB.1 Tests 1, 2, and 3. Regular user accounts are not given access to the Admin or Appliance Console, by default.

### 2.3.5.3 Consistent Security Attributes (FMT\_MSA\_EXT.5)

#### TSS Assurance Activities

##### Assurance Activity AA-FMT\_MSA\_EXT.5-ASE-01

*The evaluator shall review the TSS and in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur. If the TOE does not allow contradictory policy to exist, the evaluator shall verify that this assertion has been made in the TSS and that justification is provided to support the assertion.*

#### Summary

Section 7.1.26 *FMT\_MSA\_EXT.5 Consistent security attributes* of [ST] provides the following description:

- 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.

Section 7.1.26 also points to section 7.1.1 *ESM\_ACD.1 Access control policy definition* for further details on the Computer Policy and User Policy.

#### Guidance Assurance Activities

##### Assurance Activity AA-FMT\_MSA\_EXT.5-AGD-01

*If the TOE requires manual intervention in order to resolve contradictory policy data, the evaluator shall review the operational guidance in order to verify that it provides a summary of contradictory policy situations and the steps that must be taken in order to resolve them. If the TOE's policy engine prevents such contradictions, the evaluator shall review the operational guidance in order to verify that it describes how the TSF reconciles any contradictory policy data (such as different rules simultaneously allowing and denying a certain behavior).*

#### Summary

The TOE does not require manual intervention to resolve contradictory policy data, as the policy data is separate and distinct for each individual user and computer. As mentioned in the [CCGUIDE] section *Security Functionality subsection Enterprise Security Management*,

*" Imprivata supports multiple Computer Policies and User Policies. One Computer Policy is assigned to each managed endpoint and one User Policy is assigned to each user."*

This section also states that,

*"... in the evaluated configuration, only the password authentication mechanism is allowed as an authentication mechanism... The authentication mechanism for a user is defined in each User Policy."*

Lastly, the section outlines that the TOE maintains user accounts and authentication data in its database. Users of the managed endpoints and of the Imprivata Admin Console are validated against this database of users, which ensures that no policy collisions occur.

## Test Assurance Activities

### Assurance Activity AA-FMT\_MSA\_EXT.5-ATE-01

*The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST. If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators. This feature shall be tested in conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.*

#### Summary

Test 1 was performed with the intention of showing the TOE's enforcement of policies so that it prevents contradictions. A User Policy and a Computer Policy were created, and the "Desktop Access Authentication Restrictions" section of the Computer Policy was modified to only allow Fingerprint authentication.

This is the only contradiction that can be actively applied to two enabled policies, and the Computer Policy is given precedent to decide the allowed authentication methods over the User Policy.

The TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur. Due to this, FMT\_MSA\_EXT.5.2 is implicitly satisfied as it is impossible to have inconsistencies to detect.

### 2.3.5.4 Specification of Management Functions (FMT\_SMF.1)

## TSS Assurance Activities

### Assurance Activity AA-FMT\_SMF.1-ASE-01

*The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available.*

#### Summary

Section 7.1.27 *FMT\_SMF.1 Specification of management functions* of [ST] describes in Table 21 "Security management functions" lists the management functions that are available in the evaluated configuration including the administrative role attributes associated with each function. The evaluator verified the management functions listed in Table 21 with those in Table 10 "Management functions" provided in FMT\_SMF.1 and determined they are the same.

## Guidance Assurance Activities

### Assurance Activity AA-FMT\_SMF.1-AGD-01

*The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.*

#### Summary

The [ST] section 7.1.27 *FMT\_SMF.1 Specification of management functions* provides Table 21 *Security management functions*, which summarizes the available management functions. The section also states that the Super Administrator role can perform all management functions and the Delegated Administrator role must have the administrator role attribute specified in Table 21.

[CCGUIDE] section *Administrator Roles (Delegated Administration)* provides tables that list the attributes that are available for administrators. These tables list all of the management functions listed in Table 21 of the [ST]. Based on Table 21 of [ST] and the tables in section *Administrator Roles (Delegated Administration)*, subsection *Administrator Operations* of the [CCGUIDE], the evaluator compiled the following table:

**Table 5: ESM PM PP Management Functions**

SFR	Management Activities	Guidance	Purpose
ESM_ACD.1	Creation of policies	<p>[CCGUIDE] <b>Policies</b> table entries: Create/Edit User Policy, Delete User Policy, Assign User Policy</p> <p>Update Computer Policy, Delete Computer Policy</p> <p>Update Computers, Delete Computers, Assign Computer Policy</p> <p>Performed via the Admin Console and instructions are provided in section <i>Computers and Computer Policy</i> and <i>Users and User Policy</i></p>	The ability to create user and computer policies.
ESM_ACT.1	Transmission of policies	<p>[CCGUIDE] <b>Policies</b> table entry: Create/Edit User Policy, Delete User Policy, Assign User Policy</p> <p><b>Users</b> table entry: Update Computers Delete Computers, Assign Computer Policy</p> <p>Performed via the Admin Console and instructions are also provided in this table entry.</p>	Assign policies
ESM_ATD.1	Definition of object attributes. Association of attributes with objects.	<p>[CCGUIDE] <b>Users</b> table entry: Update Computers, Delete Computers, Assign Computer Policy</p> <p>Performed via the Admin Console and instructions are also provided in this table entry.</p>	Define and assign object attributes

SFR	Management Activities	Guidance	Purpose
ESM_ATD.2	<p>Definition of subject attributes.</p> <p>Association of attributes with subjects.</p>	<p>[CCGUIDE] <a href="#">d</a>, <b>Users</b> table entry: Add/Edit Users</p> <p>Performed via the Admin Console and instructions are provided in sections <i>Administrator Roles (Delegated Administration)</i>.</p>	Define and assign subject attributes
ESM_EAU.2	<p>Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)</p>	<p>[CCGUIDE] <a href="#">d</a>, <b>Users</b> table entries: Add/Edit Users Delete Users</p> <p>Performed via the Admin Console and instructions are provided in sections <i>Administrator Roles (Delegated Administration)</i>.</p>	Add and delete users
ESM_EID.2	<p>Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)</p>	<p>[CCGUIDE] <a href="#">d</a>, <b>Users</b> table entries: Add/Edit Users Delete Users</p> <p>Performed via the Admin Console and instructions are provided in sections <i>Administrator Roles (Delegated Administration)</i>.</p>	Add and delete users
FAU_SEL.1	<p>Configuration of auditable events</p>	<p>[CCGUIDE] <a href="#">d</a>, <b>Properties</b> table entry: Update System Properties</p> <p>Performed via the Admin Console and instructions are provided in sections <i>Manage Audit Records</i> and <i>Audit Record Maintenance</i>.</p>	The ability to define system operations and maintenance including selecting auditable events
FAU_SEL_EXT.1	<p>Configuration of auditable events for defined external entities</p>	<p>[CCGUIDE] <a href="#">d</a>, <b>Properties</b> table entry: Update System Properties</p> <p>Performed via the Admin Console and instructions are provided in sections <i>Manage Audit Records</i> and <i>Audit Record Maintenance</i>.</p>	The ability to define system operations and maintenance including selecting auditable events

SFR	Management Activities	Guidance	Purpose
FAU_STG_EXT.1	Configuration of external audit storage location	[CCGUIDE] <a href="#">d</a> , <b>Properties</b> table entry: Maintain Audit Log  Performed via the Admin Console and instructions are provided in section <i>Secure Copy Protocol for Audit File Data</i> .	The ability to maintain the audit log including archiving (e.g., sending to external audit log storage) and deleting.
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).	[CCGUIDE] <a href="#">d</a> , Chapter <i>Administrator Roles (Delegated Administration)</i> , <b>Policies</b> table entry: Create/Edit User Policy entry  Performed via the Appliance Console and instructions are provided in section <i>User Lockout Policy</i> .	Configure authentication failures.
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	[CCGUIDE] <a href="#">d</a> , <b>Users</b> table entry: Add/Edit Users  Performed via the Admin Console and instructions are provided in sections <i>Administrator Roles (Delegated Administration)</i> .	Manage subject security attributes.
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products	[CCGUIDE] <a href="#">d</a> , <ul style="list-style-type: none"> <li>• <b>Users</b> table entry: Assign Computer Policy</li> <li>• <b>Policies</b> table entry: Create/Edit User Policy, Assign User Policy</li> <li>• <b>Properties</b> table entry: Maintain Audit Log</li> <li>• <b>Policies</b> table entry: Update Computer Policy</li> <li>• <b>Properties</b> table: Update System Properties</li> </ul> Performed via the Admin Console and instructions are provided throughout the [CCGUIDE] <a href="#">d</a> .	The ability to configure the behavior of the TOE system.
FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF	(Not applicable)	Not applicable

SFR	Management Activities	Guidance	Purpose
	shall respond if any inconsistencies are detected (if applicable)		
FMT_SMR.1	Management of the users that belong to a particular role	<p>[CCGUIDE] <a href="#">📄</a>, <b>Users</b> table entries: Create/Edit Administrator Roles Delete Administrator Roles Add/Edit Users</p> <p>Performed via the Admin Console and instructions are provided in section <i>Administrator Roles (Delegated Administration)</i>.</p>	User role management
FTA_TAB.1	Maintenance of the banner	<p>[CCGUIDE] <a href="#">📄</a>, <b>Properties</b> table entry: Update System Properties entry</p> <p>Performed via the Admin Console and instructions are provided in section <i>Managing System Settings</i>, subsection <i>Banner</i>.</p>	Configure the advisory banner.
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	<p>[CCGUIDE] <a href="#">📄</a>, <b>Properties</b> table entries: Maintain Audit Log and/or Update System Properties</p> <p>Performed via the Admin Console or Appliance Console and instructions for configuring trusted path are provided in sections <i>Server Configuration</i>, <i>Administrator Roles (Delegated Administration)</i></p>	Configure trusted channel for TOE communications with other IT products (e.g., external audit log storage, syslog server)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	<p>[CCGUIDE] <a href="#">📄</a>, <b>Properties</b> table entry: Update System Properties</p> <p>Performed via the Appliance Console and instructions for configuring trusted path are provided in sections <i>Server Configuration</i> and <i>Administrator Roles (Delegated Administration)</i></p>	Configure trusted paths for the Admin Console and Appliance Console.

The evaluator verified all of the management functions that can be performed against the TSF are documented in the [CCGUIDE] [📄](#) and sufficient guidance is provided on how to perform these functions.



## Test Assurance Activities

### Assurance Activity AA-FMT\_SMF.1-ATE-01

*The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they and accomplish the documented capability*

#### Summary

All management functions listed in [ST] Table 10 were tested throughout the [DTR].

The evaluator listed example logs from testing for each required management function in FMT\_MOF.1. Access to the TOE TSFIs are only available to administrators.

## 2.3.5.5 Security Management Roles (FMT\_SMR.1)

### TSS Assurance Activities

#### Assurance Activity AA-FMT\_SMR.1-ASE-01

*The evaluator shall review the TSS to determine the roles that are defined for the TOE. The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined.*

#### Summary

Section 7.1.28 *FMT\_SMR.1 Security roles* of [ST] provides the following description for user roles:

- The Admin Console supports the Super Administrator and Delegated Administrator roles.
  - The Super Administrator role, which contains all administrator role attributes, cannot be edited or deleted and can perform all administrative operations available from the Admin Console. All other roles available from the Admin Console are subordinate to the Super Administrator role.
  - The Delegated Administrator role, which is subordinate to the Super Administrator role, whose capabilities are defined by administrator role attributes assigned by either a user with the Super Administrator role or a Delegated Administrator role with the Create/Edit Admin Administrator Roles attribute. Each Delegated Administrative role also has a unique name.
- The Appliance Console supports the Super Administrator and Administrator roles.
  - The Super Administrator role only has one account and cannot be modified or deleted. This role can perform all administrative operations on the Appliance Console including appliance backup/restore, installation of updates and upgrades, distribution of updates, change network settings, and manage system logs.
  - The Administrator role has one account and cannot be modified or deleted. This role performs a subset of the Super Administrative operations on the Appliance Console including appliance backup, change network settings, and manage system log.

The evaluator also determined that the roles defined by this SFR are consistently referenced when discussion how management authorization are determined.

### Guidance Assurance Activities

#### Assurance Activity AA-FMT\_SMR.1-AGD-01

*The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted.*

## Summary

The [ST] section 7.1.28 FMT\_SMR.1 Security roles states that the management authority is role-based with the following roles:

- The Admin Console supports the following roles:
  - Super Administrator: one account that cannot be modified or deleted
  - Delegated Administrator
- The Appliance Console supports the following roles:
  - Super Administrator: one account that cannot be modified or deleted
  - Administrator: one account that cannot be modified or deleted and performs a subset of the Super Administrative operations

The [CCGUIDE] section Administrator Roles (Delegated Administration) states that the TOE's Admin Console supports the ability to assign users to roles. In the section, the guidance specifies step-by-step instructions for establishing the role operations and defining their administration role. The steps for assigning a user to a role are as follows:

1. In the Imprivata Admin Console, go to the gear icon and select **Administrator roles**.
2. Select an existing role or click **Add Role**.
3. When selecting Add Role, Choose the role the new Administrator role will be based on, and click **Next**.
4. Specify a **Role Name**.
5. Select the **operations** this role can perform.
6. Select the **users and sites** this role can manage.
7. **Add users** to this new role.
8. Click **Save**.

As step 7 points out, new users are added to the various defined/created roles through this process of delegation. As these users would be assigned within the Admin Console, these users would be considered "Delegated Administrators". The evaluator determines that this is sufficient evidence of the guidance articulating the TOE's ability to assign various users to roles. Section *Administrator Levels* states that there can be any number of users assigned to an administrator role and that all administrator roles are created from the Super Administrator role. Section *The Super Administrator* indicates that there is only one Super Administrator role and it cannot be edited or deleted. The Super Administrator can perform all operations, and all other administrator roles are subordinate to the Super Administrator role.

## Test Assurance Activities

### Assurance Activity AA-FMT\_SMR.1-ATE-01

*The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.*

## Summary

The assurance activities for this SFR were tested in FIA\_USB.1 Tests 1, 2, and 3. These tests show that administrative management functions are available for creating, defining and assigning new roles.

Note that roles are only differentiated between users and administrators, as a user account is only for logging into endpoint agents and not for TOE management.

## 2.3.6 Protection of the TSF (FPT)

### 2.3.6.1 Protection of Stored Credentials (FPT\_APW\_EXT.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FPT\_APW\_EXT.1-ASE-01

*The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT\_SKP\_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.*

## Summary

Section 7.1.29 *FPT\_APW\_EXT.1 Protection of stored credentials* of [ST] provides the following description:

- Authentication data (i.e., Admin Console passwords, Enterprise user passwords, SSH client passwords) are encrypted by the TOE using the database symmetric encryption key to obscure the data prior to storing in the database (non-volatile memory). The TOE provides no interface to view these passwords in plaintext.
- Authentication data (i.e., Appliance Console passwords) are obscured using a salted hash and the obscured data are saved in a password file. The TOE provides no interface to view these passwords in plaintext.

## Guidance Assurance Activities

##### Assurance Activity AA-FPT\_APW\_EXT.1-AGD-01

*There are no operational guidance activities for this SFR.*

## Summary

There are no operational guidance activities for this SFR.

## Test Assurance Activities

##### Assurance Activity AA-FPT\_APW\_EXT.1-ATE-01

*The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.*

## Summary

The authentication data from the Admin Console, Enterprise user, and SSH client for external audit storage are all encrypted by the TOE using the database symmetric encryption key to obscure data prior to storing in the database. The authentication data from the Appliance Console is obscured using a salted hash and saved to a password file.

The evaluator verified that the TOE does not provide any interface to access the Operating System console or the filesystem. The only interfaces available for admin and non-admin users are the Admin Console and the Appliance Console, and the audit records which are transmitted out of the TOE boundary. Therefore, the test case to cover this assurance activity was limited to check that passwords are not shown in plaintext in any of the available management functions for credential management, and that the password values are not included in the audit records for any event.

Indeed, Test 1 was performed with the intent of verifying that passwords are not available to be viewed in plaintext from any interface. This was shown by authenticating into each interface and showing that the password is not shown in the logs or in the user settings, even for the superadmin user.

## 2.3.6.2 Protection of Secret Key Parameters (FPT\_SKP\_EXT.1)

### TSS Assurance Activities

#### Assurance Activity AA-FPT\_SKP\_EXT.1-ASE-01

*The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.*

## Summary

Section 7.1.30 *FPT\_SKP\_EXT.1 Protection of secret key parameters* of [ST] provides the following description:

- The following data is stored in cleartext on the TOE 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

### Guidance Assurance Activities

#### Assurance Activity AA-FPT\_SKP\_EXT.1-AGD-01

*There are no operational guidance or testing activities for this SFR.*

## Summary

There are no operational guidance activities for this SFR.

## Test Assurance Activities

No assurance activities defined.

### 2.3.6.3 Reliable time stamps (FPT\_STM.1)

## TSS Assurance Activities

### Assurance Activity AA-FPT\_STM.1-ASE-01

*The evaluator shall check the TSS in order to determine that it discusses the TOE's inclusion of a system clock.*

## Summary

Section 7.1.31 *FPT\_STM.1 Reliable time stamps* of [ST] [\[1\]](#) states that the TOE's OS provides reliable time stamp capabilities used by the rest of the TOE.

## Guidance Assurance Activities

### Assurance Activity AA-FPT\_STM.1-AGD-01

*The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the operational guidance instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.*

## Summary

[CCGUIDE] [\[1\]](#) section *Configure the Enterprise Settings* provides information about both setting the time and unchecking the NTP Server option. Specifically, it mentions that NTP servers are not allowed in a Common Criteria configuration and the NTP option should be unchecked in the Network Services page and the time and date set manually within the Appliance Configuration Wizard. The disabling of NTP is also mentioned in the *Before You Begin* subsection of the *Establish The Enterprise* section.

## Test Assurance Activities

### Assurance Activity AA-FPT\_STM.1-ATE-01

*The evaluator shall determine through the evaluation of operational guidance how the TOE initializes and initiates the clock. The evaluator shall then follow those instructions to set the clock to a known value, and observe that the clock monotonically increments in a reliable fashion (comparison to a reference timepiece is sufficient). Through its exercise of other TOE functions, the evaluator shall confirm that the value of the timestamp is used appropriately. If the TOE supports multiple protocols for establishing a connection with an NTP server, the evaluator shall perform this test using each supported protocol claimed in the operational guidance.*

## Summary

The purpose of this test was to show the modification of the TOE's clock settings and to show that the TOE's clock accurately increments. The evaluator verified this by setting the system clock to 1 hour and 10 minutes ahead of the current time during testing. The TOE accurately displayed these changes, and audit logs also showed the new time successfully.

## 2.3.7 TOE access (FTA)

### 2.3.7.1 TSF-initiated termination (FTA\_SSL.3)

#### TSS Assurance Activities

##### Assurance Activity AA-FTA\_SSL.3-ASE-01

*The evaluator shall check the TSS in order to determine that it discusses how inactivity is handled for remote administrative sessions*

#### Summary

Section 7.1.32 *FTA\_SSL.3 TSF-initiated termination* of [ST] discusses how inactivity is handled for remote administrative sessions as follows:

- The TOE terminates the remote sessions of both UIs (i.e., 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.
- Configuration of inactivity time interval is discussed in FMT\_SMF.1

#### Guidance Assurance Activities

##### Assurance Activity AA-FTA\_SSL.3-AGD-01

*The evaluator shall also check the operational guidance in order to verify that it describes how to set the idle time threshold.*

#### Summary

[CCGUIDE] section *Setting the Imprivata Admin Console Session Timeout* describes how to set the Admin Console session timeout setting. To configure this setting from the Admin Console, the admin selects the gear icon > **Settings**. On the Settings page, they go to **Imprivata Admin Console session timeout** and then configure the time for the value (up to 90 minutes).

Section *Setting the Imprivata Appliance Console Session Timeout* describes how to set the Appliance Console session timeout setting. From the Appliance Console, the admin selects **System** page > **Settings** tab. They will then go to **Auto Logout Idle Time (Minutes)** and select a value between zero (timeout disabled) and 600 (ten hours). The default is five minutes. There is also the auto logout idle time. Auto logout is the period of time that the Imprivata Appliance Console sits idle before automatically logging out the last administrative user and requiring a fresh login. The auto logout time for the appliance console can be set up to 600 minutes.

#### Test Assurance Activities

##### Assurance Activity AA-FTA\_SSL.3-ATE-01

*The evaluator shall test this capability by following the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.*

## Summary

The evaluator tested various inactivity timeouts on the Appliance and Admin Consoles. The minimum and maximum values differed between the two TSFIs, with the Appliance Console range being 1-600 minutes and the Admin Console range being 5-90 minutes. Both TSFI's minimum and maximum inactivity timeout periods were tested, along with another 30 minute timeout. All timeouts produced the necessary logs and the TOE closed the sessions successfully.

## 2.3.7.2 User-initiated termination (FTA\_SSL.4)

### TSS Assurance Activities

#### Assurance Activity AA-FTA\_SSL.4-ASE-01

*The evaluator shall check the TSS in order to determine that it discusses the ability of an administrator to terminate their own session.*

## Summary

Section 7.1.33 *FTA\_SSL.4 User-initiated termination* of [ST] provides the following description:

- The TOE allows administrators to terminate remote sessions of both 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.

### Guidance Assurance Activities

#### Assurance Activity AA-FTA\_SSL.4-AGD-01

*The evaluator shall check the operational guidance in order to verify that it describes how an administrator can terminate their own administrative session for each administrative interface that is supported by the TOE.*

## Summary

The [CCGUIDE] subsections *Setting the Imprivata Appliance Console Session Timeout* and *Setting the Imprivata Admin Console Session Timeout* within section *Administrator Roles (Delegated Administration)* states that the TOE allows administrators to terminate their own sessions at any time for both the Appliance and Admin Consoles (logout) within their respective NOTE sections in the guidance documentation.

### Test Assurance Activities

#### Assurance Activity AA-FTA\_SSL.4-ATE-01

*The evaluator shall test this capability by establishing a session with the TOE using an administrative interface. The evaluator then follows the operational guidance to exit or log off of the session and observes that the session has been terminated. If applicable, the evaluator shall repeat this test for each administrative interface that is supported by the TOE.*



## Summary

The evaluator successfully established sessions to both the Appliance and Admin Consoles as an administrative user. After the connection, the evaluator manually logged off of both TSFIs. It was verified that the TOE closed each session successfully and recorded the required logs.

### 2.3.7.3 TOE Access Banner (FTA\_TAB.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FTA\_TAB.1-ASE-01

*The evaluator shall check the TSS in order to determine that it discusses the ability of the TSF to display a configurable banner prior to administrator authentication.*

## Summary

Section 7.1.34 *FTA\_TAB.1 Default TOE access banners* of [ST] states that the TOE displays an administrator-configurable advisory warning message (a.k.a. banner) on both the Admin Console and the Appliance Console prior to administrator authentication.

#### Guidance Assurance Activities

##### Assurance Activity AA-FTA\_TAB.1-AGD-01

*The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured*

## Summary

Section *Banner* of [CCGUIDE] provides guidance on how to configure the banner message for the Administrator and Appliance Consoles. The banner is displayed above the username and password fields on the interface. The banner is configured via the Admin Console and displayed above the username and password fields. [CCGUIDE] section *Banner* provides step-by-step directions for configuring the banner, as follows:

1. In the Imprivata Admin Console, go to the **gear icon > Settings**.
2. In the section **Administrator login message**, enter an advisory warning message. 500 characters maximum.
3. Select a duration:
  - 7 days
  - 14 days
  - 30 days
  - 90 days
  - Always show message
4. Click **Save**.

#### Test Assurance Activities

##### Assurance Activity AA-FTA\_TAB.1-ATE-01

*If the banner is not displayed by default, the evaluator shall configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists. If applicable, the evaluator will also attempt to use the functionality to modify the TOE access banner as per the standards defined in FMT\_SMF.1 and verify that the TOE access banner is appropriately updated.*

### Summary

After confirmation that no message was showing at the login screen for the Admin or Appliance Consoles, the evaluator created a test message to be displayed and viewed this on both consoles. Further testing was able to verify that the message display timeframe is followed accurately by the TOE, and the message no longer displays after that timeframe limit has been reached.


## 2.3.7.4 TOE Session Establishment (FTA\_TSE.1)

### TSS Assurance Activities

#### Assurance Activity AA-FTA\_TSE.1-ASE-01

*The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined.*

### Summary

Section 7.1.35 *FTA\_TSE.1 TOE session establishment* of [ST]  states that Administrators can deny session establishment for all users, except Super Administrators, based on day, time, duration, and user role. 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.

### Guidance Assurance Activities

#### Assurance Activity AA-FTA\_TSE.1-AGD-01

*The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.*

### Summary

Section *TOE Access* of the [CCGUIDE]  states

*" In addition, administrators can deny session establishment for all users, except for Super Administrators, based on day, time, and duration. "*

Chapter *Managing System Settings* section *Lockdown Status* provides the information for denying session establishment for all users (except Super Administrators). The section provides the following step-by-step instructions for configuring the setting:

1. In the Imprivata Admin Console, go to the **gear icon > Settings**.
2. In the section **System lockdown**, select a lockdown schedule and duration from the drop-down menu.
3. Click **Save**.

The section also provides information on the effect of the shutdown on the various roles of the TOE.

- **Administrators and Super Administrators:** Users with Administrator privileges cannot access the Imprivata Admin Console while the system is locked. Super Administrators are not locked out.
- **Users:** Users who are not authorized for Offline Authentication can continue to work only until the next refresh interval.<sup>2</sup> The next time the user's agent contacts the Imprivata server, the user's session is terminated. Users who are not logged in cannot log in while the system is locked.

## Test Assurance Activities

### Assurance Activity AA-FTA\_TSE.1-ATE-01

*The evaluator shall test this capability by first fully establishing a session to the TOE. The evaluator then follows the operational guidance to configure the TOE so that that access is denied based on a specific value of the attribute. The evaluator shall then attempt to establish a session in contravention to the attribute setting (for instance, the location is denied based upon the time of day). The evaluator shall observe that the session establishment attempt fails.*

#### Summary

The system lockdown option was tested on the Agent with settings that were deemed sufficient for the testing being applied in the Admin Console. A lockdown was set for 4 PM for a 1-hour duration, and an attempt was made at that time to access the TOE and verify that access was not granted. Testing shows that login was not successful during the lockdown period, as expected. Logs were also correctly recorded for the TSF management function of modifying the system settings and the denial of the user session.

## 2.3.8 Trusted path/channels (FTP)

### 2.3.8.1 Inter-TSF Trusted Channel (FTP\_ITC.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FTP\_ITC.1-ASE-01

*The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.*

#### Summary

Section 7.1.36 *FTP\_ITC.1 Inter-TSF trusted channel* of [ST] provides the following description.

- The TOE provides trusted communications between itself and the external audit server over TLS, the external audit log storage over SSH, and agents over HTTPS. The TOE also remotely stores audit data at the the first two locations.
  - Communication with the external audit server: The TOE initiates and protects this communication with TLS v1.1 and 1.2 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.

<sup>2</sup> Offline Authentication is disabled in the evaluated configuration.

- Communication with the external audit log storage: The TOE initiates and protects this communication with SSHv2 provided by Apache SSHD. The TOE contains and uses the external SSH server's public key to provide assured identification of the external audit log storage.
- The TOE receives inbound connections from the agent over an HTTPS connection provided by the Apache HTTPS Server. The TOE's HTTPS server supports TLS 1.2 protocol, which are provided by Apache NSS.

## Guidance Assurance Activities

### Assurance Activity AA-FTP\_ITC.1-AGD-01

*The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.*

#### Summary

The evaluator examined section *Server Configurations* of [CCGUIDE] and determined that it provides instructions for setting up both the external audit server and the external audit log storage as well as communications with the agent.

Subsection *Trusted Path/Channels* of the [CCGUIDE] contains the following table:

**Table 6: Imprivata Protocol Support Table**

Protocol	Initiator
HTTPS (TLS 1.2)	Imprivata Admin Console to Imprivata
	Imprivata Appliance Console to Imprivata
	Imprivata agent to Imprivata
SSHv2	Imprivata to external audit log storage
TLS 1.2	Imprivata to external audit server (syslog)

This table directly correlates with the IT entities specified in the [ST]. Using the above table as a guide, the following statements showcase the guidance's statements on configuring SSH for the external audit log storage, configuring TLS for the external audit server, and HTTPS for the Imprivata Agent. The evaluator will also highlight if a service is non-configurable when applicable.

First of all, section *Install Common Criteria Feature Flag* describes the installation image called "enableAccessControlNIAP-2022-09-12.ipm" which perform the necessary steps to configure the TOE in the evaluated configuration, "CC mode". This includes restricting the SSH algorithms to only those claimed in the ST. Likewise, it also restricts the TLS versions claimed in the ST.

#### Communication with the Agent

Communication with the Agent is via HTTPS which is implemented by the TOE's Apache HTTP server and does not require configuration by the administrator. However, in [CCGUIDE] section *More on the Imprivata Agent*, it states that when the agent contacts the Imprivata appliance for the first time (enrollment), the appliance sends the agent a unique 128-bit identifier over an HTTPS connection that the agent securely stores. This key allows the Imprivata appliance to uniquely identify the agent when the agent contacts it. When the agent contacts the appliance when no user is logged into the endpoint (for example, during a refresh interval), the agent uses its unique key to identify itself to the Imprivata appliance after the HTTPS connection is established.

### Communication with the external audit log storage

This communication channel uses SSH to provide an SCP connection. As stated above, the "CC mode" restricts the SSH algorithms to those supported in the evaluated configuration. In addition, sections *Add SCP Server* and *Configure SCP for Audit Records* contain step-by-step instructions for both adding and configuring the SCP server. It also states that the user (i.e., administrative user) needs to configure the appliance's SSH public key authentication by copying and pasting the public key into the trusted hosts configuration of the SCP server. In a NOTE below the two aforementioned sections, the guidance states that the SSH public key is set by default, does not require manual configuration, and rejects all other encryption algorithms.

### Communication with the syslog server

This communication channel uses TLS. For TLS, section *Server Configurations* of the [CCGUIDE] provides information on how to configure TLS and manage TLS certificates for the syslog server. Once the correct certificates are in place, [CCGUIDE] section *Remote Syslog Server* provides step-by-step instructions for enabling the remote syslog server for TLS and RFC 5425 compliance.

Regarding broken connections, the [CCGUIDE] section *External Audit Log Storage* states the following should a connection be unintentionally broken:

*" If the connection fails during the transfer or the external audit log storage is unavailable, Imprivata OneSign retains the log files and attempts to transfer them at the next interval. When configured for on-demand transfers, Imprivata OneSign transfers audit records in log files to the external audit log storage at the request of the administrator. "*

and

*" 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. "*

## Test Assurance Activities

### Assurance Activity AA-FTP\_ITC.1-ATE-01

The evaluator shall also perform the following tests:

- *Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.*
- *Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.*
- *Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- *Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.*

Further assurance activities are associated with the specific protocols.

For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.

## Summary

For Test 1, the evaluator confirmed that communications using TLS, SSH, and HTTPS were tested throughout the evaluation. The evaluator setup these connections using the guidance documentation before proceeding, and verified that these connections were successful.

Test 2 has the purpose of verifying that these connections can actually be initiated by the TOE or an authorized IT entity. The evaluator was able to confirm this in other testing.

FAU\_STG\_EXT.1 tests the SSH and TLS protocols with our external audit storage server and syslog server. Both protocols were also tested in their respective SFRs, with SSH being tested in FCS\_SSH\_EXT.1 and TLS/HTTPS being tested in FCS\_TLS\_EXT.1. The HTTPS protocol was tested in FCS\_TLS\_EXT.1 where the TOE was configured as a TLS server. Specifically, Tests 1, 2b, and all of 3b show the connection with the TOE initiated as a TLS server via HTTPS.

Tests 3 and 4 were ran with the purpose of showing the data not being sent across any of the communications in plaintext, as well as the action taken when each connection is physically interrupted. The evaluator verified that the data sent across these communication channels are protected, and that no data is sent across these channels in the event of a disconnect until the communication protocol was able to be successfully reestablished. This was tested for SSH, TLS, and HTTPS.

### 2.3.8.2 Trusted path (FTP\_TRP.1)

#### TSS Assurance Activities

##### Assurance Activity AA-FTP\_TRP.1-ASE-01

*The evaluator shall repeat the assurance activity for FTP\_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration.*

#### Summary

Section 7.1.37 *FTP\_TRP.1 Trusted path* of [ST][\[1\]](#) provides the following description:

- The TOE supports two remote web browser-based administrative interfaces: Admin Console and Appliance Console.
- The browsers connects the TOE using HTTPS with TLS 1.2. 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.

#### Guidance Assurance Activities

##### Assurance Activity AA-FTP\_TRP.1-AGD-01

*The evaluator shall repeat the assurance activity for FTP\_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration.*

#### Summary

The evaluator examined section *Trusted Path/Channels* of [CCGUIDE][\[1\]](#), which states:

*" Administrators externally manage Imprivata via the Imprivata Admin Console and Imprivata Appliance Console on a web browser, over HTTPS with 1.2. "*

As stated in AA-FTP\_ITC.1-AGD-01, section *Install Common Criteria Feature Flag* describes the installation image called "enableAccessControlNIAP-2022-09-12.ipm" which perform the necessary steps to configure the TOE in the evaluated configuration, "CC mode". This includes restricting the TLS versions claimed in the ST.

Also, [CCGUIDE] states that HTTPS protocol is implemented by the TOE's Apache HTTP server and does not require configuration by an administrator. In addition, section *Enterprise Security Management* states that the Admin Console and Appliance Console both support password authentication as its is the only authentication mechanism.

## Test Assurance Activities

### Assurance Activity AA-FTP\_TRP.1-ATE-01

*The evaluator shall repeat the assurance activity for FTP\_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration.*

### Summary

For Test 1, the HTTPS communication protocol was thoroughly tested throughout the course of the evaluation. This trusted communication path was tested specifically in FCS\_TLS\_EXT.1 Tests 1, 2b, and all of 3b.

Test 2 was also thoroughly tested throughout the course of the evaluation with remote user authentication via the OneSign Agent. ESM and FIA testing, specifically ESM\_ACT.1 Test 1 and FIA\_AFL.1 Test 3, show the successful and unsuccessful authentication process on the remote agent.

Tests 3 and 4 were ran with the purpose of showing the data not being sent across any of the communications in plaintext, as well as the action taken when each connection is physically interrupted. The evaluator verified that the data sent across these communication channels are protected, and that no data is sent across these channels in the event of a disconnect until the communication protocol was able to be successfully reestablished.

Test 3 was also thoroughly tested throughout the course of the evaluation with initial user authentication via the OneSign Agent. Initial authentication is required prior to TSF access, and the available management functions for the Agent were covered in FMT\_MOF.1.



## 2.4 Security Assurance Requirements

There are no assurance activities for Security Assurance Requirements.

# A Appendixes

## A.1 References

CC	<b>Common Criteria for Information Technology Security Evaluation</b>
Version	3.1R5
Date	April 2017
Location	<a href="http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf">http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf</a>
Location	<a href="http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf">http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf</a>
Location	<a href="http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf">http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf</a>
CCEVS-TD0042	<b>Removal of Low-level Crypto Failure Audit from PPs</b>
Date	2018-06-15
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0042">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0042</a>
CCEVS-TD0055	<b>Move FTA_TAB.1 to Selection-Based Requirement</b>
Date	2015-07-30
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0055">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0055</a>
CCEVS-TD0066	<b>Clarification of FAU_STG_EXT.1 Requirement in ESM PPs</b>
Date	2015-10-08
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0066">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0066</a>
CCEVS-TD0079	<b>RBG Cryptographic Transitions per NIST SP 800-131A Revision 1</b>
Date	2018-06-15
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0079">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0079</a>
CCEVS-TD0573	<b>Update to FCS_COP and FCS_CKM in ESM PPs</b>
Date	2021-01-29
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0573">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0573</a>
CCEVS-TD0574	<b>Update to FCS_SSH in ESM PPs</b>
Date	2021-01-29
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0574">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0574</a>
CCEVS-TD0576	<b>FTP_ITC and FTP_TRP Updated</b>
Date	2021-01-29
Location	<a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576</a>

CCEVS-TD0621	<b>Corrections to FCS_TLS_EXT.1 in ESM PPs</b> Date 2022-02-02 Location <a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0621">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0621</a>
CCEVS-TD0794	<b>Correction to FCS_SSH_EXT.1.7 Test 2</b> Date 2023-10-03 Location <a href="https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0794">https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0794</a>
CCGUIDE	<b>Imprivata OneSign Version 7.9 Common Criteria Administration Guide</b> Version v21 Date 2023-09-12 File name <a href="agd/CommonCriteria_AdminGuide_Draft21.pdf">agd/CommonCriteria_AdminGuide_Draft21.pdf</a>
CEM	<b>Common Methodology for Information Technology Security Evaluation</b> Version 3.1R5 Date April 2017 Location <a href="http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf">http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf</a>
DTR	<b>Imprivata OneSign version 7.9 Detailed Test Report</b> Version 1.0 Date 2023-10-04 File name <a href="ate/ImprivataOneSign_DTR.v1.0.pdf">ate/ImprivataOneSign_DTR.v1.0.pdf</a>
ESMPMPP	<b>Standard Protection Profile for Enterprise Security Management Policy Management</b> Version 2.1 Date 2013-10-24 Location <a href="https://www.niap-ccevs.org/MMO/PP/pp_esm_pm_v2.1.pdf">https://www.niap-ccevs.org/MMO/PP/pp_esm_pm_v2.1.pdf</a>
ESMPMPPv2.1	<b>Protection profile Enterprise Security Management - Policy Management Version 2.1</b> Version 2.1 Date 2013-11-21 Location <a href="https://www.niap-ccevs.org/MMO/pp/pp_esm_pm_v2.1.pdf">https://www.niap-ccevs.org/MMO/pp/pp_esm_pm_v2.1.pdf</a>
RFC2818	<b>HTTP Over TLS</b> Author(s) E. Rescorla Date 2000-05-01 Location <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a>
SP800-90A-Rev1	<b>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</b> Date 2015-06-24 Location <a href="https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final">https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final</a>
ST	<b>Imprivata OneSign Version 7.9 Security Target</b> Version 1.3 Date 2023-10-06 File name <a href="ase/OneSign_ST_1.3.pdf">ase/OneSign_ST_1.3.pdf</a>

## A.2 Glossary

### **Augmentation**

The addition of one or more requirement(s) to a package.

### **Authentication data**

Information used to verify the claimed identity of a user.

### **Authorised user**

A user who may, in accordance with the SFRs, perform an operation.

### **Class**

A grouping of CC families that share a common focus.

### **Component**

The smallest selectable set of elements on which requirements may be based.

### **Connectivity**

The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

### **Dependency**

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

### **Deterministic RNG (DRNG)**

An RNG that produces random numbers by applying a deterministic algorithm to a randomly selected seed and, possibly, on additional external inputs.

### **Element**

An indivisible statement of security need.

### **Entropy**

The entropy of a random variable  $X$  is a mathematical measure of the amount of information gained by an observation of  $X$ .

### **Evaluation**

Assessment of a PP, an ST or a TOE, against defined criteria.

### **Evaluation Assurance Level (EAL)**

An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

### **Evaluation authority**

A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

### **Evaluation scheme**

The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

### **Exact conformance**

a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the requirements in the Security Requirements section of the PP, and potentially requirements from Appendices of the PP. While iteration is allowed, no additional requirements (from the CC parts 2 or 3) are allowed to be included in the ST. Further, no requirements in the Security Requirements section of the PP are allowed to be omitted.

**Extension**

The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

**External entity**

Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

**Family**

A grouping of components that share a similar goal but may differ in emphasis or rigour.

**Formal**

Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Guidance documentation**

Documentation that describes the delivery, preparation, operation, management and/or use of the TOE.

**Identity**

A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

**Informal**

Expressed in natural language.

**Object**

A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

**Operation (on a component of the CC)**

Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

**Operation (on an object)**

A specific type of action performed by a subject on an object.

**Operational environment**

The environment in which the TOE is operated.

**Organisational Security Policy (OSP)**

A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.

**Package**

A named set of either functional or assurance requirements (e.g. EAL 3).

**PP evaluation**

Assessment of a PP against defined criteria.

**Protection Profile (PP)**

An implementation-independent statement of security needs for a TOE type.

**Random number generator (RNG)**

A group of components or an algorithm that outputs sequences of discrete values (usually represented as bit strings).

**Refinement**

The addition of details to a component.

**Role**

A predefined set of rules establishing the allowed interactions between a user and the TOE.

**Secret**

Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

**Secure state**

A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.

**Security attribute**

A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

**Security Function Policy (SFP)**

A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.

**Security objective**

A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.

**Security Target (ST)**

An implementation-dependent statement of security needs for a specific identified TOE.

**Seed**

Value used to initialize the internal state of an RNG.

**Selection**

The specification of one or more items from a list in a component.

**Semiformal**

Expressed in a restricted syntax language with defined semantics.

**ST evaluation**

Assessment of an ST against defined criteria.

**Subject**

An active entity in the TOE that performs operations on objects.

**Target of Evaluation (TOE)**

A set of software, firmware and/or hardware possibly accompanied by guidance.

**TOE evaluation**

Assessment of a TOE against defined criteria.

**TOE resource**

Anything useable or consumable in the TOE.

**TOE Security Functionality (TSF)**

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

**Transfers outside of the TOE**

TSF mediated communication of data to entities not under control of the TSF.

**True RNG (TRNG)**

A device or mechanism for which the output values depend on some unpredictable source (noise source, entropy source) that produces entropy.

**Trusted channel**

A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

**Trusted path**

A means by which a user and a TSF can communicate with necessary confidence.

**TSF data**

Data created by and for the TOE, that might affect the operation of the TOE.

**TSF Interface (TSFI)**

A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.

**User**

See external entity

**User data**

Data created by and for the user, that does not affect the operation of the TSF.