

Document #:

Status: DRAFT

Version: 2.1

# SunSpec Cybersecurity Certification

## Release 2024 Test Procedure



Copyright © SunSpec Alliance 2024. All Rights Reserved.

All other copyrights and trademarks are the property of their respective owners.

## **License Agreement and Copyright Notice**

This document and the information contained herein is provided on an "AS IS" basis and the SunSpec Alliance DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This document may be used, copied, and furnished to others, without restrictions of any kind, provided that this document itself may not be modified in anyway, except as needed by the SunSpec Technical Committee and as governed by the SunSpec IPR Policy. The complete policy of the SunSpec Alliance can be found at [sunspec.org](http://sunspec.org).

Prepared by the SunSpec Alliance

4040 Moorpark Avenue, Suite 110

San Jose, CA 95117

Website: [sunspec.org](http://sunspec.org)

Email: [info@sunspec.org](mailto:info@sunspec.org)

## **About the SunSpec Alliance**

The SunSpec Alliance is a trade alliance of developers, manufacturers, operators, and service providers together pursuing open information standards for the distributed energy industry. SunSpec standards address most operational aspects of PV, storage, and other distributed energy power plants on the smart grid, including residential, commercial, and utility-scale systems, thus reducing cost, promoting innovation, and accelerating industry growth.

Over 180 organizations are members of the SunSpec Alliance, including global leaders from Asia, Europe, and North America. Membership is open to corporations, non-profits, and individuals. For more information about the SunSpec Alliance, or to download SunSpec specifications at no charge, visit [sunspec.org](https://sunspec.org).

## **About the SunSpec Specification Process**

SunSpec Alliance specifications are initiated by SunSpec members to establish an industry standard for mutual benefit. Any SunSpec member can propose a technical work item. Given sufficient interest and time to participate, and barring significant objections, a workgroup is formed and its charter is approved by the board of directors. The workgroup meets regularly to advance the agenda of the team.

The output of the workgroup is generally in the form of a SunSpec Interoperability Specification. These documents are considered to be normative, meaning that there is a matter of conformance required to support interoperability. The revision and associated process of managing these documents is tightly controlled. Other documents are informative, or make some recommendation with regard to best practices, but are not a matter of conformance. Informative documents can be revised more freely and more frequently to improve the quality and quantity of information provided.

SunSpec Interoperability Specifications follow a lifecycle pattern of: DRAFT, TEST, APPROVED, and SUPERSEDED.

For more information or to download a SunSpec Alliance specification, go to <https://sunspec.org/about-sunspec-specifications/>.

# 1 Revision History

Version	Date	Comments
0.1	22-11-23	Initial draft based on Lumian contribution
0.2	23-01-11	Draft for comments
0.3	23-03-13	Incorporated feedback
0.4	23-03-31	Incorporated feedback
0.5	23-06-03	Incorporate feedback from review meetings
0.6	23-06-06	Removed log retention requirement, updated ICS, updated factory reset test case
0.7	23-06-07	Renamed Test Manual to IXIT
0.8	23-06-08	Cleanup references, add DER/LOG/BV-05
1.0	23-07-11	Integrate remaining public comments
2.1	24-03-05	First draft of Release 2024

## 2 Contents

1	Revision History .....	4
2	Contents .....	5
3	Scope .....	7
4	References .....	8
5	Definitions and abbreviations .....	9
5.1	Definitions.....	9
5.2	Abbreviations.....	9
6	Setup preambles .....	11
6.1	Operational states .....	11
6.1.1	DER/PRE/ST-01: Basic operational state .....	11
6.1.2	DER/PRE/ST-02: Factory default state .....	11
6.2	Required Equipment .....	11
7	Test cases .....	13
7.1	Software Update .....	13
7.1.1	DER/SWUP/BV-01: Software Version .....	13
7.1.2	DER/SWUP/BV-02: Secure Updates .....	13
7.1.3	DER/SWUP/BV-03: Support of Automatic Remote Updates.....	15
7.2	Device Communication .....	15
7.2.1	DER/DCOM/BV-01: Support of Secure Communications .....	17
7.2.2	DER/DCOM/BV-02: Downgrade Prevention .....	18
7.2.3	DER/DSEC/BV-01: Minimal Interfaces .....	20
7.3	Authentication .....	21
7.3.1	DER/AUTH/BV-01: Unique Credentials .....	23
7.3.2	DER/AUTH/BV-02: Authentication .....	24
7.3.3	DER/AUTH/BV-03: Session Timeout .....	25
7.3.4	DER/AUTH/BV-04: Configurable Timeout .....	26
7.3.5	DER/AUTH/BV-05: Strong Passwords.....	27
7.3.6	DER/AUTH/BV-06: Unique Passwords .....	28
7.3.7	DER/AUTH/BV-07: Brute Force Prevention.....	29
7.3.8	DER/AUTH/BV-08: Admin Login without Brute Force Protection .....	29
	DER/AUTH/BV-08: Password Protection .....	30
7.4	Logging.....	31

7.4.1	DER/LOG/BV-01: Configuration Logs .....	32
7.4.2	DER/LOG/BV-02: Power Setting Logs .....	33
7.4.3	DER/LOG/BV-03: Power Cycle Logs .....	33
7.4.4	DER/LOG/BV-04: Remote Logs .....	34
7.4.5	DER/LOG/BV-05: Secure Logs .....	34
	Device Security .....	35
7.4.6	DER/DSEC/BV-01: Factory Reset .....	36

## 3 Scope

This document is used by SunSpec Cybersecurity Authorized Test Labs (ATLs) to conduct tests in accordance with the SunSpec Cybersecurity Certification Program (“SCCP”). This version describes the Release 2024 test procedure and ATLs can forward the results of this procedure to the SCCP Certification Body for certification consideration.

For further comments on scope, see Section 3 of SunSpec Cybersecurity Certification Release 2024 Requirements [1]

## 4 References

- [1] SunSpec Alliance, SunSpec Cybersecurity Certification Release 2024 Requirements, Version 2.0, 2024. <https://sunspec.org/specifications/>
- [2] National Security Agency Eliminating Obsolete TLS Protocol Configurations. [https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING\\_OBSOLETE\\_TLS\\_UOO197443-20.PDF](https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF)
- [3] IETF Deprecation of IKEv1 and obsoleted algorithms. <https://datatracker.ietf.org/doc/rfc9395/>
- [4] IEC 62351-9: 2023.



# 5 Definitions and abbreviations

## 5.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**Communication Capability:** a communication capability of the IUT as specified by the Manufacturer in the ICS Document.

**Endpoint:** A device or server external to the IUT that the IUT can communicate with using one of its Communication Capabilities. Examples include a test tool, a software update server, and a software developer's development computer.

**ICS Document:** Manufacturer-supplied document that describes capabilities of the device including optional configurations or extendable functionality that is able to communicate over the public Internet. The ICS ("information conformance statement") Document should be verified using the contents of the Product Manual. The ICS Document form can be found in Exhibit A.

**Logical Connections:** All electronic and user interface access points into the IUT. Examples include a physical admin panel or an SSH port open to the public Internet.

**Network Activity:** Active information (such as data packets) exchanged between the IUT and Endpoint and are recorded with a Network Traffic Monitor.

**Product Manual:** A document the Manufacturer supplies to users of the IUT to instruct the user on how to operate all publicly available features of the IUT.

**Secret:** Authentication password, private key, or other authentication credential.

**IXIT (Implementation Extra Information for Testing):** Operational Information provided by the Manufacturer that instructs Test Engineer how to perform operations not described in the Product Manual.

**Timestamp:** All logfiles must record a timestamp (DER/LOG/REQ-02: Timestamp Logs [1]) that conforms with DER/LOG/REQ-03: Timestamp Resolution [1] and DER/LOG/REQ-04: Timestamp Accuracy [1].

**Power Cycle:** A power Cycle consists of two steps: 1) Power down or remove power from a device, and 2) turn the device back on.

## 5.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AUTH      Authentication

DCOM      Device Communication

DER        Distributed energy resource

DSEC      Device security

ICS        Implementation Conformance Statement

IUT        Implementation under test (a single product SKU- product "combinations" are not allowed unless the combination has its own SKU)

SWUP    Software Update

# 6 Setup preambles

## 6.1 Operational states

### 6.1.1 DER/PRE/ST-01: Basic operational state

State of the IUT required to operate normally, including activating all Communication Capabilities.

### 6.1.2 DER/PRE/ST-02: Factory default state

State of the IUT when it comes out of the box for the first time.

## 6.2 Required Equipment

- 1 IUT (provided by the manufacturer) running a software image older than the production software image under test. If the IUT supports local software updates, a total of 2 such IUTs are needed. Note that the IUT is not to be “wiped” between test cases unless explicitly stated. Test engineers must use the same IUT(s) throughout this document.
- Enough Endpoints (provided by the manufacturer, either installed locally at the lab or as a remotely accessible server) to exercise each Communication Capability of the IUT. Such Endpoints should be as close to the production implementation as possible. Each Endpoint needs to be accessible to the test engineer so they can modify the communication security settings (e.g.- change the apache2.conf file and restart Apache). Manufacturer must supply documentation (Product Manual and/or IXIT) to instruct test engineer how to change these security settings.
- Remote Log and Incident Server (provided by the manufacturer, either installed locally at the lab or as a remotely accessible server)- an Endpoint that can receive and store log files and incident reports from the IUT. The Remote Log and Incident Server should be as close to the production implementation as possible. Note that security events may be stored in a separate file as the remote reporting timeframes for security events are more stringent than other logs.
- Remote Software Update Server (provided by the manufacturer, either installed locally at the lab or as a remotely accessible server)- an Endpoint that is able to send software updates to the IUT. The Remote Software Update Server should be as close to the production implementation as possible. Test engineer must be able to load different software update images to this server.
- 3 IUT software images (provided by the manufacturer):
  - 1) Current Image that is the current production image of the IUT and is authenticated by the manufacturer (e.g.- contains manufacturer’s signature).
  - 2) Unauthenticated Image that is the same as the Current Image but has not been authenticated by the manufacturer (e.g.- no signature).
  - 3) Modified Image that is the Current Image modified after the manufacturer authenticates (e.g.- signs) the image. The test engineer is allowed to further modify the Modified Image, if possible, for a more robust test.

- 4) Old Image that is an older version than the Current Image and is authenticated by the manufacturer. The version of each component in the Old Image should also be older than the version of each component in the Current Image.

Completed and signed ICS Document (provided by the manufacturer).

- Product Manual (provided by the manufacturer).
- IXIT (provided by the manufacturer). The Product Manual combined with the IXIT (“Manuals”) must include instructions that allow the test engineer to operate the IUT to complete each test case. Manufacturers must review each test case in this document and ensure the test engineer can perform each one by reading the instructions in the Manuals.
- IUT Functional Specification, hardware and software (provided by the manufacturer).
- Network Traffic Monitor (provided by the test lab).
- Wi-Fi scanner (provided by the test lab).
- Bluetooth scanner (provided by the test lab).
- Ethernet port scanner (provided by the test lab).
- Secrets (keys, passwords, tokens, etc.) required to successfully authenticate communications using each Communication Capability (provided by the manufacturer).
- Clock: a timekeeper able to be synchronized to UTC and display time with millisecond resolution. This clock must be synchronized to UTC when running each test case. Time recordings in test cases should be recorded in milliseconds.

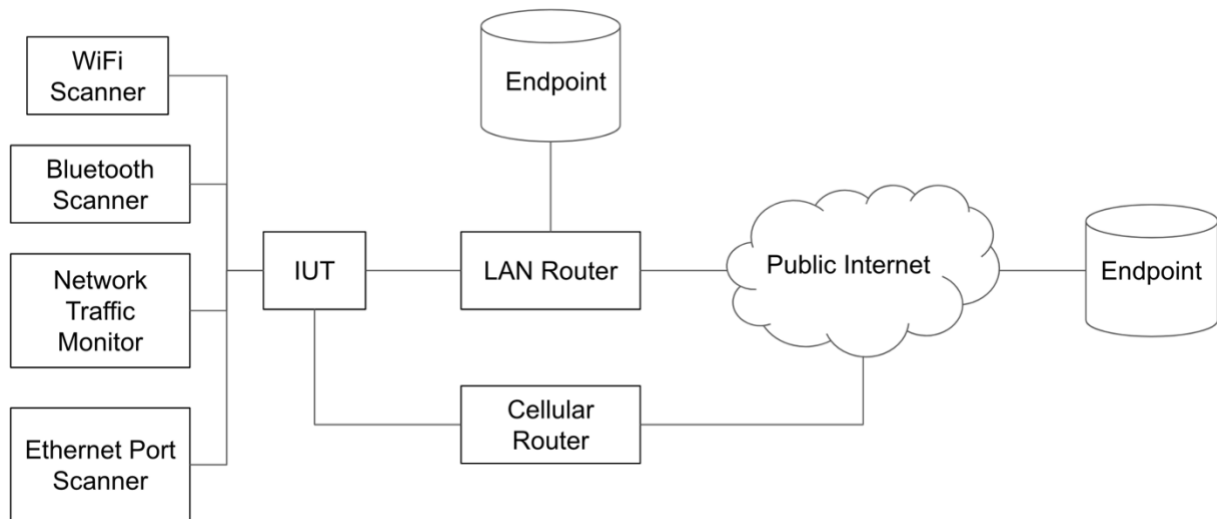


Figure 1: Block diagram of test harness.

# 7 Test cases

## 7.1 Software Update

### 7.1.1 DER/SWUP/BV-01: Software Version

#### *Test Purpose*

Verify that the IUT supports a mechanism to read the version of each component.

#### *Obligation*

Mandatory

#### *Reference*

- DER/SWUP/REQ-01: Software Updates [1]
- DER/SWUP/REQ-02: Software Version [1]

#### *Initial Condition*

- An IUT with a software image older than the current image is in its basic operational state, as defined in DER/PRE/ST-01.

#### *Test Procedure*

1. Record the software version of the IUT software following instructions in the Product Manual.
2. Record the version of each installed security and operational software component shown in Table 6-1 of DER/SWUP/REQ-01 by following instructions in the Manuals.

#### *Expected Outcome*

- The test engineer can read the software version of the image and each component shown in Table 6-1 of DER/SWUP/REQ-01.

### 7.1.2 DER/SWUP/BV-02: Secure Updates

#### *Test Purpose*

Verify the IUT verifies the authenticity and integrity of a software update image before installing it.

#### *Obligation*

Mandatory

#### *Reference*

- DER/SWUP/REQ-01: Software Updates [1]
- DER/SWUP/REQ-05: Secure Updates [1]
- DER/LOG/REQ-06: Security Logs [1]

## DER/LOG/REQ-08: Incident Reporting [1]

### *Initial Condition*

- IUT used in 7.1.1 is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive logs.
- If the IUT supports local software updates, a second IUT is in its basic operational state, as defined in DER/PRE/ST-01.

### *Test Procedure*

1. Read and record the software version of the currently installed software and every component on the IUT shown in Table 6-1 of DER/SWUP/REQ-01.
2. Load the Unauthenticated Image on the Remote Software Update Server.
3. Initiate a remote software update on the IUT and record the time.
4. Read and record the software version of the IUT's currently installed software.
5. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.1.2-1.
6. Load the Modified Image on the Remote Software Update Server.
7. Initiate a remote software update on the IUT and record the time.
8. Read and record the software version of the IUT's currently installed software.
9. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.1.2-2.

The following steps should only be executed if the IUT supports local software updates.

10. Read and record the software version of the currently installed software and every component on the second IUT.
11. Load the Unauthenticated Image on the second IUT and record the time.
12. Read and record the software version of the second IUT's currently installed software.
13. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.1.2-1a.
14. Load the Modified Image on the second IUT and record the time.
15. Read and record the software version of the second IUT's currently installed software.
16. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.2.2-2a.

### *Expected Outcome*

- The software versions in steps 4 and 8 are the same as the versions in step 1.
- The IUT is operational.
- Logfile 7.1.2-1 contains the security event in step 3.
- Logfile 7.1.2-2 contains the security event in step 7.

If the IUT supports local software updates:

- The software versions in steps 12 and 15 are the same as the versions in step 10.
- The second IUT is operational.
- Logfile 7.1.2-1a contains the security event in step 11.
- Logfile 7.1.2-2a contains the security event in step 14.

### 7.1.3 DER/SWUP/BV-03: Support of Automatic Remote Updates

#### *Test Purpose*

Verify that the IUT supports automatic remote updates for each software component.

#### *Obligation*

Mandatory

#### *Reference*

- DER/SWUP/REQ-01: Software Updates [1]
- DER/SWUP/REQ-03: Remote Updates [1]
- DER/SWUP/REQ-04: Automatic Updates [1]
- DER/LOG/REQ-06: Security Logs [1]

#### *Initial Condition*

- The IUT from 7.1.2 is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive reports from IUT.

#### *Test Procedure*

1. Load the Current Image on the Remote Software Update Server and record the time.
2. Wait 24 hours.
3. Read and record the software version of the first IUT's currently installed software and the version of each software component shown in Table 6-1 of DER/SWUP/REQ-01.

#### *Expected Outcome*

- Each version in step 3 is higher than the corresponding versions in 7.1.2 step 1.
- The IUT is operational.

### 7.1.4 DER/SWUP/BV-04: Software Downgrade Prevention

#### *Test Purpose*

Verify that the IUT rejects updates to software versions older than the currently installed versions.

#### *Obligation*

Mandatory

#### *Reference*

- DER/SWUP/REQ-07: Downgrade Prevention [1]
- DER/LOG/REQ-08: Incident Reporting [1]

#### *Initial Condition*

- The IUT from 7.1.3 is in its basic operational state, as defined in DER/PRE/ST-01.

- Remote Log and Incident Server is ready to receive reports from IUT.
- If the IUT supports local updates, the second IUT from 7.1.3 is in its basic operational state, as defined in DER/PRE/ST-01.

### *Test Procedure*

1. Load the Old Image on the Remote Software Update Server.
2. Initiate a remote software update on the IUT and record the time once the IUT is operational.
3. Record the software version of the IUT's currently installed software.
4. Wait one minute and export the logs from Remote Log and Incident Server, marking it as Logfile 7.1.4.

The following should only be completed if the IUT supports local software updates.

5. Load the Old Image on the second IUT following instructions in the Product Manual and record the time once the IUT is operational.
6. Record the software version of the second IUT's currently installed software.
7. Wait one minute and export the logs from Remote Log and Incident Server, marking it as Logfile 7.1.4a.

### *Expected Outcome*

- The software versions in step 3 and 7.1.3 step 5 are the same.
- The IUT is operational.
- Logfile 7.1.4 contains the security incident in step 2 with the correct timestamp.
- If the IUT supports local software updates, the software versions in step 6 and 7.1.3 step 4 are the same, the second IUT is operational, and Logfile 7.1.4a contains the security incident in step 5 with the correct timestamp.

## **7.1.5 DER/SWUP/BV-05: Secure Update Operations**

### *Test Purpose*

Ensure the manufacturer maintains secure operations for all processes that touch the software update functionality of the IUT.

### *Obligation*

Optional.

### *Reference*

- DER/SWUP/REQ-08: Software Provenance [1]
- IEC 62443-4-2 (information security management system)
- IEC 12207 (software development life cycle)

### *Initial Condition*

None.



### *Test Procedure*

- Confirm the software update system (including software on the IUT and the back end service) has been certified for IEC 12207 or IEC 62443-4-1 (software development lifecycle certification programs) by an organization authorized by SunSpec CCP in the past two years.

### *Expected Outcome*

- Software update system has the correct certification.

## **7.2 Device Communication**

### **7.2.1 DER/DCOM/BV-01: Support of Secure Communications**

#### *Test Purpose*

Ensure all Communication Capabilities that are accessible by the public (see DER/DCOM/REQ-01 [1] for an explanation on this) are properly secured.

#### *Obligation*

Mandatory

#### *Reference*

- DER/DCOM/REQ-01: Secure Communications [1]
- DER/DCOM/REQ-02: Downgrade Prevention [1]

#### *Initial Condition*

- The IUT from 7.1.3 is in its basic operational state, as defined in DER/PRE/ST-01.
- All Endpoints are ready to communicate with the IUT.
- Valid Secrets required to authenticate communications for each Communication Capability are installed in the IUT and all Endpoints.
- Remote Log and Incident Server is ready to receive logs.

#### *Test Procedure*

For each of the Communication Capabilities listed in Section 1 of the ICS Document that support TLS, DTLS, IPsec, or SSH, perform the following test procedure:

1. Set up the IUT so it can activate the Communication Capability.
2. Set up the Network Traffic Monitor to use the protocol listed for the Communication Capability (TLS, DTLS, IPsec, or SSH).
3. Attach the Network Traffic Monitor so it can analyze the traffic between the IUT and Endpoint corresponding to the Communication Capability.
4. Start the Network Traffic Monitor and activate the Communication Capability.
5. Record the network traffic with the Network Traffic Monitor.
6. Record the protocol and ciphersuite being used by the Communication Capability.

Note: the test for symmetric key authentication in IPSEC is simple- if the manufacturer needs to provide you with a symmetric key the IUT fails this test case.

For each of the Communication Capabilities listed in Section 1 of the ICS Document that do not support TLS, DTLS, IPsec, or SSH, perform the following test procedure:

1. Record if the Communication Capability is listed in Exhibit A of SunSpec Cybersecurity Certification Release 2024 Requirements [1].
2. If the Communication Capability requires a certification, check the appropriate website to determine if the Communication Capability has received certification.
3. If the Communication Capability has prohibited functionality listed in Exhibit A, attempt to use each prohibited functionality listed and record whether or not the functionality is capable of being used and functions correctly.

### *Expected Outcome*

- For each Communication Capability listed in Section 1 of the ICS Document that supports TLS, DTLS, IPsec, or SSH, records indicate the IUT successfully used an allowed security protocol (TLS 1.2 or higher, DTLS 1.2 or higher, IPsec Version 2 or higher, or SSH-2) that is not in Table 7-1 and a ciphersuite/key exchange algorithm/transform that is not listed in Table 6-3 or 6-4 of DER/DCOM/REQ-02.
- For each Communication Capability that does not support TLS, DTLS, IPsec, or SSH
  - 1) The Communication Capability is listed in Exhibit A of SunSpec Cybersecurity Certification Release 2024 Requirements [1].
  - 2) The Communication Capability has the required certifications (if any are required).
  - 3) The Communication Capability does not support any of the prohibited functionality listed in Exhibit A of SunSpec Cybersecurity Certification Release 2024 Requirements [1].

## **7.2.2 DER/DCOM/BV-02: Communication Downgrade Prevention**

### *Test Purpose*

Ensure the IUT does not use or downgrade to unsecure protocols, ciphersuites, key exchange algorithms, or transforms.

### *Obligation*

Mandatory

### *Reference*

- DER/DCOM/REQ-01: Secure Communications [1]
- DER/DCOM/REQ-02: Downgrade Prevention [1]
- DER/LOG/REQ-08: Incident Reporting [1]
- National Security Agency Eliminating Obsolete TLS Protocol Configurations [2]
- IETF Deprecation of IKEv1 and obsoleted algorithms [3]

### *Initial Condition*

- The IUT from 7.2.1 is in its basic operational state, as defined in DER/PRE/ST-01.
- Endpoint configuration files are accessible and writable by test engineer according to the IXIT.
- Remote Log and Incident Server is ready to receive logs.

## Test Procedure

For each of the Communication Capabilities listed in Section 1 of the ICS document, perform the following test procedure:

1. Set up the IUT so it can activate the Communication Capability.
2. For each deprecated protocol listed in Table 7-1 associated with the Communication Capability's protocol:
  - a. Configure the Endpoint so that it will request to use only the deprecated protocol.
  - b. Attach the Network Traffic Monitor so it can confirm that the Endpoint is requesting the deprecated protocol.
  - c. Activate the Communication Capability and record the time.
  - d. Wait one minute and export the Remote Log and Incident Server logs, marking it as Logfile 7.2.2-1 with the Communication Capability index number and the deprecated protocol.
3. If the Communication Capability supports TLS 1.2, configure the Endpoint so that it will request to use only TLS 1.2. For each for each of the rows in Table 6-2 of DER/DCOM/REQ-02 do the following:
  - a. Configure the Endpoint so that it will request to use only the deprecated ciphersuite/key exchange algorithm.
  - b. Attach the Network Traffic Monitor so it can record that the Endpoint is requesting the deprecated ciphersuite/key exchange algorithm.
  - c. Activate the Communication Capability and record the time.
  - d. Wait one minute and export the Remote Log and Incident Server logs, marking it as Logfile 7.2.2-2 with the Communication Capability index number and algorithm name.

If the Communication Capability uses IPSEC, configure the Endpoint so that is uses the production IPSEC settings and for each for each of the rows in Table 6-3 of DER/DCOM/REQ-02 do the following:

- a. Configure the Endpoint so that it will request to use only the deprecated transforms.
- e. Attach the Network Traffic Monitor so it can record that the Endpoint is requesting the deprecated transforms.
- b. Activate the Communication Capability and record the time.
- c. Wait one minute and export the Remote Log and Incident Server logs, marking it as Logfile 7.2.2-3 with the Communication Capability index number and transform name.

Protocol	Deprecated Versions
TLS	SSL 1.0
TLS	SSL 2.0
TLS	SSL 3.0
TLS	TLS 1.0
TLS	TLS 1.1
DTLS	DTLS 1.0
DTLS	DTLS 1.1

IPSEC	IKEv1
IPSEC	<b>IKEv2 with symmetric key authentication</b>
SSH	SSH-1

*Table 7-1: Deprecated security protocols.*

### *Expected Outcome*

- Endpoint(s) correctly request(s) the deprecated protocol, ciphersuite, key exchange algorithm, or transform.
- IUT rejects all connections.
- Logfiles 7.2.2-1, 7.2.2-2, and 7.2.2-3 contain (with the correct timestamp) the security event that happened right before the Logfile was exported.

### **7.2.3 DER/DSEC/BV-01: Minimal Interfaces**

#### *Test Purpose*

Ensure the IUT has no unused interfaces or ports.

#### *Obligation*

Mandatory

#### *Reference*

- DER/DSEC/REQ-01: Minimal Interfaces [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.

#### *Test Procedure*

1. Observe the IUT and review the ICS Document.
2. Record any hardware interfaces on the IUT not listed in the ICS document.
3. Test all hardware interfaces not listed in the ICS document using the appropriate tester for the hardware interface (e.g.- Bluetooth scanner for a Bluetooth interface).
4. For each hardware interface listed in Section 2 of the ICS Document, test for the existence of any of the logical ports listed in [Table 7-2](#) that are not listed in Section 2 of the ICS document.

<b>Interface/Port</b>	<b>Test Procedure</b>
Ethernet	Connect the Ethernet port scanner to see how many of the possible 65,535 ports are open.
WiFi Station	Check if active using the WiFi scanner

Interface/Port	Test Procedure
WiFi Access Point	Check if active using the WiFi scanner
WiFi Bridge	Check if active using the WiFi scanner
WiFi Router	Check if active using the WiFi scanner
Bluetooth	Check if active using the Bluetooth scanner

Table 7-2: List of hardware interfaces to scan for open ports.

*Expected Outcome*

- All active interfaces and ports are listed in the ICS Document Section 2.
- All hardware interfaces not listed in the ICS Document Section 2 are disabled.

**7.2.4 DER/DSEC/BV-04: Support of Secure Boot**

*Test Purpose*

Ensure the IUT implements secure boot.

*Obligation*

Mandatory.

*Reference*

- DER/DSEC/REQ-05: Secure Boot [1]

*Initial Condition*

None.

*Test Procedure*

Review the questions 8 and 9 of the ICS Document.

*Expected Outcome*

Manufacturer answered “Yes” in questions 8 and 9 of the ICS Document.

**7.2.5 DER/DSEC/BV-02: Support of Root of Trust Protection**

*Test Purpose*

Ensure the IUT prevents modification of all root-of-trust data.

*Obligation*

Mandatory.

## Reference

- DER/DSEC/REQ-03: Root of Trust Protection [1]

## Initial Condition

- The IUT from 7.2.3 is in its basic operational state, as defined in DER/PRE/ST-01.

## Test Procedure

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

1. If possible, obtain the endpoint certificate from the Network Traffic Monitor records.
2. If possible, obtain the location of the root certificates by observing the configuration settings of the software library responsible for the Communication Capabilities security (e.g.- OpenSSL).
  - a. If the root certificate location cannot be found from the configuration settings, review the IXIT and Product Manual to get the location.
3. If the endpoint certificate is available, find the root certificate that is used to verify the certificate and try to modify it.
  - a. If no endpoint certificate is available, try to modify every root certificate that can be used by the Communication Capability software library (e.g.- if the software library uses certificates stored in a folder, modify every certificate in the folder).

Review question 10 of the ICS Document.

## Expected Outcome

- The root certificate used by each Communication Capability cannot be modified by any user except the highest level of access control (e.g.- root).
- The manufacturer answers “Yes” on question 10 of the ICS Document.

## 7.2.6 DER/DSEC/BV-03: Support for Root of Trust Extension

### Test Purpose

Ensure the IUT provides a secure mechanism for the manufacturer or entity approved by the manufacturer to add additional pieces of root of trust data.

### Obligation

Mandatory.

## Reference

- DER/DSEC/REQ-04: Root of Trust Extension [1]

## Initial Condition

- The IUT from 7.2.5 is in its basic operational state, as defined in DER/PRE/ST-01.

### *Test Procedure*

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

1. Review the IXIT and Product Manual to determine how to use the mechanism for adding a root of trust to the IUT.
2. Ensure the mechanism is listed in Section 1 of the ICS Document.
3. Use the mechanism to add a new root of trust to the IUT.
4. Add a new certificate, derived from the new root of trust, to the endpoint used to test the Communication Capability.
5. Activate the Communication Capability.

Note: secure boot root of trust does not require an extension capability.

### *Expected Outcome*

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

- Root of trust extension mechanism is listed in Section 1 of the ICS Document.
- Root of trust extension mechanism successfully completes.
- Communication Capability connects to the endpoint with the new certificate.

## **7.3 Authentication**

### **7.3.1 DER/AUTH/BV-01: Unique Credentials**

#### *Test Purpose*

Ensure each user account in the IUT requires separate credentials.

#### *Obligation*

Mandatory

#### *Reference*

- DER/AUTH/REQ-01: Unique Credentials [1]
- DER/LOG/REQ-06: Security Logs [1]

#### *Initial Condition*

- The IUT is in its original factory setting state, as defined in DER/PRE/ST-02.

#### *Test Procedure*

1. Create a first user account on the IUT with its own unique ID and authentication credential. Record the time.
2. If the IUT allows creation of more than one user account, create a second user account with a different ID and authentication credential. Record the time.
3. Attempt to login to each created account. Record the time of each login attempt.

### *Expected Outcome*

- Test engineer can successfully create a user account with a unique ID with a unique credential.
- If the IUT allows creation of more than one user account, test engineer successfully creates a second user account with a unique ID and credential.
- Test engineer successfully logs into each created account.

### **7.3.2 DER/AUTH/BV-02: Authentication**

#### *Test Purpose*

Ensure the IUT authenticates all logical connections, including the physical administration panel should one exist.

#### *Obligation*

Mandatory

#### *Reference*

- DER/AUTH/REQ-02: Authentication [1]
- DER/LOG/REQ-06: Security Logs [1]
- DER/LOG/REQ-08: Incident Reporting [1]
- DER/LOG/REQ-11: Panel Logs [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive reports from IUT.

#### *Test Procedure*

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

1. Set up the IUT and appropriate Endpoint with the proper credentials using the Manuals.
2. Activate the Communication Capability and record the time.
3. Set up the IUT and appropriate Endpoint with the proper credentials replaced by false credentials using the Manuals.
4. Activate the Communication Capability and record the time.
5. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.3.2 with the Communication Capability index.

If there is a physical admin panel:

6. Attempt to access the panel with correct credentials and record the time.
7. Attempt to access the panel with incorrect credentials and record the time.
8. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.3.2a.



### *Expected Outcome*

- IUT accepts all connections and login attempts in step 2 and 6.
- IUT rejects all connections and login attempts in step 4 and 7.
- Logfiles 7.3.2(a) contain the failed login security event (with the correct timestamp) right before the Logfile was exported.

### **7.3.3 DER/AUTH/BV-03: Session Timeout**

#### *Test Purpose*

Ensure every authenticated session times out after inactivity.

#### *Obligation*

Mandatory

#### *Reference*

- DER/AUTH/REQ-03: Session Timeout [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Endpoints and IUT are set up to communicate with proper authentication credentials.

#### *Test Procedure*

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

1. Note the timeout time of the Communication Capability in Section 1 of the ICS Document.
2. Start the Communication Capability.
3. For Communication Capabilities that require human operation:
  - a. Pause operations for the timeout time and then attempt to continue operations.
4. For machine-based communication capabilities:
  - b. Observe the communications using the Network Traffic Monitor.
  - c. Stop communications for the timeout time (if possible).
  - d. Record Network Activity observed by the monitor, including all packets with a timestamp, for a time equal to twice the Communication Capability's current timeout time.

#### *Expected Outcome*

- For Communication Capabilities that require human operation, attempts to continue operations after the timeout time fail and the user is prompted to re-authenticate.
- For machine Communication Capabilities, analyze the Network Activity records. If there is a period of time greater than the timeout time that shows no network traffic, confirm that the Communication Capability goes through the authentication process

again before any more network traffic is attempted. Note- some Communication Capabilities use continuous communications and will never time out.

### 7.3.4 DER/AUTH/BV-04: Configurable Timeout

#### *Test Purpose*

Ensure the session timeout time can be configured by the end user.

#### *Obligation*

Mandatory

#### *Reference*

- DER/AUTH/REQ-04: Configurable Timeout [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Endpoints are set up to communicate with proper authentication credentials.

#### *Test Procedure*

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

1. Modify the timeout time of the Communication Capability and record the time.
2. Start the Communication Capability.
3. For Communication Capabilities that require human operation:
  - a. Pause operations for the new timeout time and then attempt to continue operations.
4. For machine-based Communication Capabilities:
  - a. Observe the communications using the Network Traffic Monitor.
  - b. Stop communications for the timeout time (if possible).
  - c. Record Network Activity observed by the monitor, including all packets with a timestamp, for a time equal to twice the Communication Capability's current timeout time.

#### *Expected Outcome*

- For Communication Capabilities that require human operation, attempts to continue operations fails and the user is prompted to re-authenticate.
- For machine Communication Capabilities, analyze the Network Activity records. If there is a period of time greater than the new timeout time that shows no network traffic, confirm that the Communication Capabilities goes through the authentication process again before any more network traffic is attempted.

### 7.3.5 DER/AUTH/BV-05: Strong Passwords

#### Test Purpose

Ensure all passwords are strong and the IUT notifies the user if a weak password is entered.

#### Obligation

Mandatory for password authentication mechanisms only (if the IUT does not use passwords for authentication, skip this test case).

#### Reference

- DER/AUTH/REQ-05: Strong Passwords [1]
- DER/LOG/REQ-06: Security Logs [1]

#### Initial Condition

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive reports from IUT.

#### Test Procedure

For each of the Communication Capabilities listed in Section 1 of the ICS document that use password for authentication, and for the IUT admin panel (if any), perform the following test procedure:

1. Attempt to change the password of the Communication Capability to one that contains at least one letter, one number, and one non-alphanumeric character, but only 7 total characters. Note the response and record the time.
2. Attempt to change the password of the Communication Capability to one that contains at least one letter, one number, one non-alphanumeric character, and a total of 64 characters. Note the response and record the time
3. Attempt to use a password between 8 and 64 characters that has only numbers and non-alphanumeric characters. Note the response and record the time.
4. Attempt to use a password between 8 and 64 characters that has only letters and non-alphanumeric characters. Note the response and record the time.
5. Attempt to use a password between 8 and 64 characters that has only letters and numbers. Note the response and record the time.
6. Record any factory-installed password (either on the device or in the Product Manual)
7. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.3.5.

Format	Example	Requirement
Less than 8 characters	pass1!	Fail
64 characters	01234567890123456789012345 67890123456789012345678901 2345678901p!	Pass
No numbers	password!	Fail

No non-alphanumeric characters	password1	Fail
--------------------------------	-----------	------

*Table 7-3: Unsecure password formats*

*Expected Outcome*

- IUT rejects the password in step 1, 3, 4 and 5 and notifies the user of the password requirements.
- IUT accepts the password in step 2.
- Recorded passwords on the IUT have 8 or more characters with at least one number, one letter, and one non-alphanumeric character.
- Logfile 7.3.5 contains the security event in step 1, 3, 4, and 5 with the correct timestamp.

**7.3.6 DER/AUTH/BV-06: Unique Passwords**

*Test Purpose*

Ensure the IUT uses unique passwords or prompts the user to create a new password on first login.

*Obligation*

Mandatory for password authentication mechanisms only (if the IUT does not use passwords for authentication skip this test case).

*Reference*

- DER/AUTH/REQ-06: Unique Passwords [1]

*Initial Condition*

- The IUT is in its factory default state, as defined in DER/PRE/ST-02.

*Test Procedure*

1. Check the ICS Document and Product Manual to see if the IUT has a unique password installed at the factory.
2. If yes, check to see if the password is shown on the IUT (either a label or on a screen).
3. If no, log in to the IUT according to the manufacturer's instructions.

*Expected Outcome*

- If the manufacturer states the IUT has a factory-installed unique password, the password is not shown on the IUT.
- If there is common password installed in all instances of the IUT or the factory-installed unique password is shown on the IUT, the test engineer is prompted to create a new password on first login.

### 7.3.7 DER/AUTH/BV-07: Brute Force Prevention

#### *Test Purpose*

Ensure the IUT prevents brute force password attacks.

#### *Obligation*

Mandatory for single-factor password authentication mechanisms only (if the IUT does not use passwords for authentication, or the device uses a second authentication factor in addition to password authentication, skip this test case).

#### *Reference*

- DER/AUTH/REQ-07: Brute Force Prevention [1]
- DER/LOG/REQ-8: Incident Reporting [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- At least one user has set up an account with password and no other factor of authentication.
- Remote Log and Incident Server is ready to receive reports from IUT.

#### *Test Procedure*

1. Attempt to log in to the IUT at least 10 times using an incorrect password.
2. Record the time when IUT triggers account lockout.
3. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.3.7.
4. Try password login 4 minutes after account lockout.

#### *Expected Outcome*

- IUT locks login for at least 5 minutes after a maximum of 10 incorrect password attempts.
- Logfile 7.3.7 contains the security event in step 1 with the correct timestamp.
- Test engineer is not able to login in step 4.

### 7.3.8 DER/AUTH/BV-08: Admin Login without Brute Force Protection

#### *Test Purpose*

Ensure the IUT supports at least one network-accessible admin account that does not utilize brute force prevention.

#### *Obligation*

Mandatory.

#### *Reference*

- DER/AUTH/REQ-09: Admin Login without Brute Force Protection [1]
- DER/LOG/REQ-06: Security Logs [1]

- DER/LOG/REQ-08: Incident Reporting [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- An admin account with remote access to the IUT is set up with authentication credentials using an authentication mechanism that does not rely solely on a password. This may be set up by the manufacturer or the test engineer using documentation supplied by the manufacturer.

#### *Test Procedure*

1. Attempt to log in to the IUT remotely with the admin account at least 20 times using incorrect credentials.
2. Immediately after step 1, attempt to log in to the IUT remotely with the admin account using the correct credentials. Record the time.

#### *Expected Outcome*

- Test engineer is able to successfully log in with the admin account in step two.

### **7.3.9 DER/AUTH/BV-09: Password Protection**

#### *Test Purpose*

Ensure the IUT does not reveal passwords.

#### *Obligation*

Mandatory for password authentication mechanisms only (if the IUT does not use passwords for authentication, skip this test case).

#### *Reference*

- DER/AUTH/REQ-08: Password Protection [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- At least one user has set up a password.

#### *Test Procedure*

1. Study the Product Manual and record each mechanism for accessing user profile data.
2. Log into the IUT at the highest access control security level.
3. Look up passwords utilizing each mechanism.
4. Study the Product Manual and record all instances when the IUT requires a user to enter a password.
5. Attempt to enter a password for each instance.

### *Expected Outcome*

- All passwords are obfuscated and cannot be viewed, including when a password is being entered.

### **7.3.10 DER/AUTH/BV-10: Support for Credential Revocation**

#### *Test Purpose*

Ensure the IUT rejects authorization credentials that have been revoked or have expired.

#### *Obligation*

Mandatory

#### *Reference*

- DER/DCOM/REQ-03: Credential Revocation [1]

#### *Initial Condition*

- The IUT from 7.3.9 is in its basic operational state, as defined in DER/PRE/ST-01.
- All Endpoints are ready to communicate with the IUT with proper authorization credentials.
- Remote Log and Incident Server is ready to receive logs.

#### *Test Procedure*

For each of the Communication Capabilities listed in Section 1 of the ICS Document, perform the following test procedure:

1. Review the IXIT to determine how the IUT checks for revoked credentials.
2. Execute revocation of the credential on the endpoint.
3. Activate the Communication Capability and record the time.
4. Wait one minute and export the logs from the Remote Log and Incident Server, marking it as Logfile 7.3.10 with the Communication Capability index.

### *Expected Outcome*

- IUT rejects all connections and/or login attempts in step 3.
- All 7.3.10 Logfiles contain the failed communication or login security event (with the correct timestamp) right before the Logfile was exported.

### **7.3.11 DER/AUTH/BV-11: Support of Credential Provenance**

#### *Test Purpose*

Ensure the IUT's authentication credentials are created and protected securely in conformance with IEC 62351-9:2023 [4].

#### *Obligation*

Mandatory

### *Reference*

- DER/DCOM/REQ-04: Credential Provenance [1]

### *Initial Condition*

None

### *Test Procedure*

1. Ask manufacturer for IEC 62351-9 certification.
2. For each of the Communication Capabilities listed in Section 1 of the ICS Document:
  - Review the IXIT to determine the location and storage mechanism of the credential on the IUT.
  - Attempt to read the credential from the highest level of access.

### *Expected Outcome*

- Manufacturer has received IEC 62351-9 certification for its credential provisioning process within the last two years.
- No credentials can be read.

## **7.4 Logging**

### **7.4.1 DER/LOG/BV-01: Configuration Logs**

#### *Test Purpose*

Ensure the IUT logs changes to configuration.

#### *Obligation*

Mandatory

#### *Reference*

- DER/LOG/REQ-05: Configuration Logs [1]

#### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive logs.

#### *Test Procedure*

1. View the configuration settings from Section 4 of the ICS document.
2. Randomly select 10 settings.
3. For each randomly selected setting, record the old value, change the configuration value, record the new value, and record the time.
4. Export the IUT logs. This is Logfile 7.4.1.



### *Expected Outcome*

- Each configuration change in step 3 is shown in Logfile 7.4.1 with the correct timestamp.

## **7.4.2 DER/LOG/BV-02: Power Setting Logs**

### *Test Purpose*

Ensure the DER device stores power-related power configuration changes.

### *Obligation*

Mandatory

### *Reference*

- DER/LOG/REQ-09: Power Setting Logs [1]

### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive logs.

### *Test Procedure*

1. For each of the Power Protocols listed in Section 7 of the ICS Document, perform the following test procedure:
  - a. Obtain a list of power configuration settings from the ICS Document.
  - b. Change each power configuration setting on the IUT and record the time of each configuration change.
2. Export the IUT logs. This is Logfile 7.4.2.

### *Expected Outcome*

- Logfile 7.4.2 shows each power configuration change event with the correct timestamp.

## **7.4.3 DER/LOG/BV-03: Power Cycle Logs**

### *Test Purpose*

Ensure the DER device logs Power Cycles.

### *Obligation*

Mandatory

### *Reference*

- DER/LOG/REQ-10: Power Cycle Logs [1]

### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.

### *Test Procedure*

1. Remove power from the device and record the time.
2. Power the device again and record the time.
3. Export the logs in the IUT. This is Logfile 7.4.3.

### *Expected Outcome*

- Logfile 7.4.3 should contain the Power Cycle event with the correct timestamps.

## **7.4.4 DER/LOG/BV-04: Remote Logs**

### *Test Purpose*

Ensure the IUT sends logs to a remote central repository at least once a day.

### *Obligation*

Mandatory

### *Reference*

- DER/LOG/REQ-06: Security Logs [1]
- DER/LOG/REQ-07: Remote Logs [1]

### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive logs.

### *Test Procedure*

1. Wait 24 hours.
2. Export the logs from Remote Log and Incident Server. This is Logfile 7.4.4.

### *Expected Outcome*

- Logfile 7.4.4 shows the following events with the correct timestamp:
  - 1) Successful software updates from 7.1.3
  - 2) Creation of user accounts and successful logins from 7.3.1
  - 3) Successful connections from 7.3.2
  - 4) Timeout configuration change from 7.3.4
  - 5) Password change attempts from 7.3.5
  - 6) Successful admin login from 7.3.8

## **7.4.5 DER/LOG/BV-05: Secure Logs**

### *Test Purpose*

Ensure access to DER device logs require access credentials.

### *Obligation*

Mandatory

### *Reference*

- DER/LOG/REQ-01: Secure Logs [1]

### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.

### *Test Procedure*

1. Record all the methods for viewing IUT logs.
2. For each method, attempt to view IUT logs without authentication.
3. For each method, attempt to view the IUT logs with false credentials.
4. Record all the methods for editing IUT logs.
5. For each method, attempt to edit IUT logs without authentication.
6. For each method, attempt to edit the IUT logs with false credentials.

### *Expected Outcome*

- All attempts to view or edit IUT logs fail.

## **7.4.6 DER/LOG/BV-06: Log Overflow Warning**

### *Test Purpose*

Ensure the manufacturer sends a warning to a remote server before it runs out of log storage space.

### *Obligation*

Mandatory.

### *Reference*

- DER/LOG/REQ-12: Log Retention [1]

### *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Remote Log and Incident Server is ready to receive logs and messages.

### *Test Procedure*

1. Review the IXIT and Product Manual to determine what happens when log storage runs low and how to fill up IUT log storage (e.g.- adding a file that will take up space).
2. Force the IUT into a state that is 100 bytes below 10% remaining log storage space.
3. Record the time.
4. Repeatedly perform an action that triggers a log entry (e.g.- changing a password, security setting, or activating a communication capability).
5. Export the logs from Remote Log and Incident Server. This is Logfile 7.4.6.

### *Expected Outcome*

- Logfile 7.4.6 contains a warning message that is timestamped after the recorded time.

## 7.4.7 DER/LOG/BV-07: Log Retention

### *Test Purpose*

Ensure the manufacturer stores network activity logs at least 7 days and all other logs at least 90 days.

### *Obligation*

Mandatory.

### *Reference*

- DER/LOG/REQ-13: Log Retention [1]

### *Initial Condition*

None

### *Test Procedure*

1. 2 days after the Remote Logs test case, read the IUT's network activity and general logs on the Remote Log and Incident Server. This is Logfile 7.4.7.1.
2. Review questions 11 and 12 in the ICS Document

### *Expected Outcome*

- Logfile 7.4.7.1 contains the same events as contained in Logfile 7.4.2.
- Manufacturer answered "yes" to questions 11 and 12 of the ICS Document.

## 7.5 Device Security

### 7.5.1 DER/DSEC/BV-01: Factory Reset

#### *Test Purpose*

Ensure the IUT is able to reset to factory settings (DER/PRE/ST-02: Factory default state).

#### *Obligation*

Mandatory

#### *Reference*

- DER/DSEC/REQ-02: Factory Reset [1]

#### *Initial Condition*

- The IUT from 7.4 is in its basic operational state, as defined in DER/PRE/ST-01.

#### *Test Procedure*

1. Activate the factory reset function following instructions in the Product Manual.

2. Export the logs in the IUT. This is Logfile 7.5.1.

*Expected Outcome*

- IUT is back in factory mode (DER/PRE/ST-02: Factory default state).
- No user information is found on the IUT through Product Manual documented interfaces.
- All user accounts created by test engineer are no longer stored.
- All locations in ICS section 6 only contain factory data.
- Logfile 7.5.1 contains no entries from Logfile 7.4.6.

## Exhibit A

### Implementation Conformance Statement (ICS) Document

This form must be filled out by the manufacturer of the IUT. Test engineers must verify the contents of this form against the Product Manual of the IUT.

1. Does the IUT support local software updates?

2. List of all Communication Capabilities:

As a convenience, the following is a list of communication capabilities that are often overlooked:

- DNS
- NTP

Communication Capability	Security Protocol (e.g.- TLS)	Initiator (IUT/Endpoint)	Authentication Mechanism	Default Timeout (ms)

3. List of all ports and interfaces:

Logical Ports: Static port number or protocols supported.

Destination Ports: Destination port of the communication endpoint.

Hardware Interface	Logical Ports	Destination Port
Ethernet		
WiFi		
Bluetooth		

4. List all configuration settings (provide a separate document).

5. List all IEEE 2030.5-related configuration settings (provide a separate document).

6. List all locations where data is stored persistently on the IUT (provide a separate document).

7. List all power protocols. Write in protocols that are supported but are not listed

Protocol	Supported?
IEEE 2030.5	
DMP3	

8. Does the IUT support secure boot?

Yes       No

9. Is the secure boot functionality enabled by default?

Yes       No

10. Does the secure boot functionality prevent modification of the root of trust used by secure boot?

Yes       No

11. Are you capable of storing network activity logs (either on the device or Remote Incident Server) for at least 7 days?

Yes       No

12. Are you capable of storing general logs (either on the device or Remote Incident Server) for at least 90 days?

Yes       No