# Supporting Document

# Mandatory Technical Document

# PP-Module for Enterprise Session Controller (ESC)

Version: 1.0

2020-11-19

**National Information Assurance Partnership**

# Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the Common Criteria Recognition Arrangement (CCRA).

## Technical Editor:

National Information Assurance Partnership (NIAP)

## Document history:

V1.0, 19 November 2020 (Initial)

## General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of an Enterprise Session Controller (ESC).

## Field of special use:

Enterprise Session Controller (ESC).

## Acknowledgements:

The NIAP Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia supported the development of this SD.

## Table of Contents

# 1 Introduction

## 1.1 Technology Area and Scope of Supporting Document

The scope of the Enterprise Session Controller (ESC) PP-Module is to describe the security functionality of an ESC in terms of [CC] and to define functional and assurance requirements for such products.

The PP-Module is intended for use with the following Base-PP:

- Protection Profile for Network Devices (NDcPP), Version 2.2e

This SD is mandatory for evaluations that claim conformance to a PP-Configuration that includes the following PP-Module:

- PP-Module for Enterprise Session Controller (ESC), Version 1.0

As such, it defines Evaluation Activities (EAs) for the functionality described by the ESC PP-Module as well as any impacts to the NDcPP EAs that are required by the PP-Configuration.

Although EAs are defined mainly for the evaluators to follow, in general they will also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of Security Functional Requirements (SFRs), and may identify particular requirements for the content of Security Targets (STs) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

## 1.2 Structure of the Document

This document contains modifications and additions to the SD for the NDcPP to accommodate the evaluation of a network device TOE that also provides ESC functionality.

The remainder of this section introduces terminology that is relevant to ESC functionality.

Section 2 is divided into two parts. Section 2.1 lists the NDcPP SFRs that are applicable to the ESC functionality and provides instructions for whether the evaluator performs the NDcPP EAs for those SFRs as described in the NDcPP SD, or whether any additional or alternative actions are required. Section 2.2 lists the mandatory SFRs added by the ESC PP-Module and provides EAs for them.

Similar to the structure of the NDcPP SD, Sections 3-4 identify EAs for any optional, selection-based, and objective SFRs defined by the PP-Module.

Section 5 identifies EAs for any objective SFRs defined by the PP-Module.

Section 6 defines Security Assurance Requirement (SAR) EAs for the PP-Module, specifically any cases where the SAR EAs must be supplemented to ensure that the ESC portion of the TOE Security Functionality (TSF) is adequately evaluated.

## 1.3 Terminology

### 1.3.1 Glossary

For definitions of standard CC terminology, see [CC] part 1.

**Supplementary Information**

Information that is not necessarily included in the ST or operational guidance, and that may not necessarily be public. Examples of such information could be entropy analysis, or description of a cryptographic key management architecture used in (or in support of) the TOE. The requirement for any such supplementary information will be identified in the corresponding PP or PP-Module.

Reference the terminology section of [NDcPP] in addition to the terms listed below.

*Table 1: Technology Terms and Definitions*

| Term | Definition |
|---|---|
| Audit Log | A persistent record of security-relevant events such as administrative access, administrative actions performed, system failures, and the establishment and termination of remote communications. |
| Call Detail Record | A log of call metadata that can be used to determine characteristics of a call, such as its length and involved parties, without recording any of its content. |
| Call Processing | The act of translating a dialed phone number into an attempt to establish a connection with the appropriate party; this is in contrast to the actual transmission of voice/video media over a call. |
| Enterprise Session Controller | A type of network device that is responsible for establishment, processing, and termination of Voice/Video over IP (VVoIP) calls. |
| Service Provider | A third-party telecommunications company that is responsible for providing commercial service and connectivity to the worldwide telephone network. |
| Session Border Controller | A type of network device that resides on the edge of a VVoIP network that is responsible for filtering corrupted or potentially malicious traffic and preventing it from entering or leaving the network. |
| System Log | A live display of system characteristics that can be viewed on demand to diagnose system performance in real-time. This data is typically only stored for a short period of time if at all. |
| Telecommunications Device | In this PP-Module, used to refer generally to any piece of infrastructure equipment that the ESC may connect to other than a VVoIP Endpoint, which could include equipment such as a call conferencing server or Session Border Controller. |
| Trunking | The concept of connecting multiple networks together; analogous to the use of a T1 line in a legacy telephone network. |
| VVoIP Endpoint | A VVoIP-capable phone or software application that a human user can use to make or receive a voice or video call. |

### 1.3.2 Acronyms

Reference the acronyms section of [NDcPP] in addition to the acronyms listed below

*Table 2: Acronyms*

| Acronym | Meaning |
|---|---|
| **CDR** | Call Detail Record |
| **ESC** | Enterprise Session Controller |

| Acronym | Meaning |
|---|---|
| **MGCP** | Media Gateway Control Protocol |
| **NDcPP** | Collaborative Protection Profile for Network Devices |
| **OA&M** | Operations, Administration, and Management |
| **SIP** | Session Initiation Protocol |
| **VVoIP** | Voice/Video over IP |

# 2 Evaluation Activities for SFRs

The EAs presented in this section are intended to supplement those defined in the NDcPP SD.

The ESC PP-Module relies on several NDcPP SFRs to help in the implementation of its required functionality. These NDcPP SFRs are listed in this section along with any impact to how they are to be evaluated in a TOE that includes the PP-Module. This section also defines the EAs for the mandatory SFRs that are introduced in the PP-Module.

Successful completion of these EAs assists in the completion of the relevant portions of ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1, which are required to be applied to the entire TOE as per NDcPP, version 2.2e.

## 2.1 NDcPP Evaluation Activities

In addition to the EAs required by the Base-PP, the evaluator shall perform the following additional EAs to ensure that the Base-PP's security functionality is maintained by the addition of the PP-Module.

### 2.1.1 Security Audit (FAU)

#### 2.1.1.1 Security Audit Data Generation (FAU_GEN)

##### FAU_GEN.1 Audit Data Generation (Audit Log)

The evaluator shall complete the EA for FAU_GEN.1 as described in the NDcPP SD for the auditable events defined above in addition to the applicable auditable events that are defined in the NDcPP. The evaluator shall also ensure that the administrative actions defined for this PP-Module are appropriately audited.

#### 2.1.1.2 Security Audit Event Storage (FAU_STG)

##### FAU_STG.1 Protected Audit Trail Storage

There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than optional, but there is no change to how the SFR is to be implemented.

### 2.1.2 Cryptographic Support (FCS)

#### 2.1.2.1 DTLS Server Protocol (FCS_DTLSS_EXT)

##### FCS_DTLSS_EXT.1 DTLS Server Protocol without Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP SD.

##### FCS_DTLSS_EXT.2 DTLS Server Support for Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion selection-based rather than optional, but there is no change to how the SFR is to be implemented.

#### 2.1.2.2 NTP Protocol (FCS_NTP_EXT)

##### FCS_NTP_EXT.1 NTP Protocol

No additional EAs are specified for this SFR beyond what is defined in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than conditional, but there is no change to how the SFR is to be implemented.

#### 2.1.2.3 TLS Client Protocol (FCS_TLSC_EXT)

##### FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than conditional, but there is no change to how the SFR is to be implemented.

##### FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than optional, but there is no change to how the SFR is to be implemented.

#### 2.1.2.4 TLS Server Protocol (FCS_TLSS_EXT)

##### FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than conditional, but there is no change to how the SFR is to be implemented.

##### FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than optional, but there is no change to how the SFR is to be implemented.

### 2.1.3 Identification and Authentication (FIA)

#### 2.1.3.1 Authentication Using X.509 Certificates (FIA_X509_EXT)

##### FIA_X509_EXT.1 X.509/Rev Certificate Validation

No additional EAs are specified for this SFR beyond what is defined in the NDcPP SD.

##### FIA_X509_EXT.2 X.509 Certificate Authentication

No additional EAs are specified for this SFR beyond what is defined in the NDcPP SD.

##### FIA_X509_EXT.3 X.509 Certificate Requests

No additional EAs are specified for this SFR beyond what is defined in the NDcPP SD.

### 2.1.4 Protection of the TSF (FPT)

#### 2.1.4.1 Time Stamps (FPT_STM_EXT)

##### FPT_STM_EXT.1 Reliable Time Stamps

No additional EAs are specified for this SFR beyond what is defined in the NDcPP SD.

## 2.2 TOE SFR Evaluation Activities

### 2.2.1 Security Audit (FAU)

### 2.2.1.1 Security Audit Data Generation (FAU_GEN)

#### FAU_GEN.1/CDR Audit Data Generation (Call Detail Record)

*TSS*

The evaluator shall examine the TSS to ensure it describes the format of the Call Detail Records (CDRs) generated by the TOE in sufficient detail to demonstrate that the requirement is satisfied.

*Operational Guidance*

The evaluator shall examine the guidance documentation to determine that it describes the format of CDRs in sufficient detail for the reader to understand their contents and any configuration actions that are required in order for the CDRs to include the data that is mandated by this PP-Module.

*Test*

Note that these test activities may be performed in conjunction with other tests.

The evaluator shall deploy the TOE in an environment where it can be used to establish calls for a supported signaling protocol (i.e. Session Initiation Protocol (SIP), H.323). The evaluator shall place a call between two VVoIP endpoints, allow it to remain connected for three minutes, and then hang up. The evaluator shall then verify that the TOE generated CDRs for this call that contain all necessary information in the format specified by the operational guidance and that this information is accurate. The evaluator shall then place a second call where the call is transferred to a third VVoIP endpoint prior to termination.

The evaluator shall repeat this testing for each type of signaling protocol supported by the TOE.

#### FAU_GEN.1/Log Audit Data Generation (System Log)

*TSS*

The evaluator shall examine the TSS to ensure that and ensure that it mentions the system log and describes how the log is presented. Each type of entry in the system log shall be listed along with a brief description of each content field and what the sampling interval for the data is. The evaluator shall also check to make sure that every log type mandated by the PP-Module is described and that the description of the content fields contains the information required in FAU_GEN.1.2/Log.

*Operational Guidance*

The evaluator shall check the guidance documentation and ensure any configuration necessary to ensure the TOE generates the required system log is included. The evaluator shall also check that each required system log item is described in the guidance documentation along with each required content field.

*Test*

The evaluator shall perform the following tests:

Test 1 (current IP connections): First, confirm TOE is connected via IP by pinging it from a remote device. Once IP is confirmed connected, take down IP connection either by physically disconnecting network cable from the TOE's NIC; or as TOE Administrator, issue command to logically take down IP connection. Peruse system logs to confirm IP connection is down. After confirming IP connection as down, reconnect IP or logically bring up IP connection and confirm IP status as up. Repeat for each physical network interface of the TOE.

Test 2 (CPU usage): The evaluator shall use the TOE and monitor the CPU usage status over a period of 10 minutes and observe that fluctuations in CPU usage are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these fluctuations are occurring (e.g. CPU usage spikes while the TOE is establishing a call).

Test 3 (memory usage): The evaluator shall use the TOE and monitor the memory usage status over a period of 10 minutes and observe that fluctuations in memory usage are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these fluctuations are occurring (e.g. memory usage spikes while the TOE is establishing a call or downloading an update).

Test 4 (disk and file storage capacity): The evaluator shall use the TOE and monitor the disk capacity status over a period of 10 minutes and observe that fluctuations in storage capacity are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these changes are occurring (e.g. the evaluator transfers a file with a known file size to a disk partition and observes that the available space decreased by a corresponding amount).

Test 5 (fan status) (conditional): First, confirm fan is working as designed. Once fan is confirmed functioning properly, disconnect fan to shut it down. Peruse system logs to confirm fan has been reported as down. After confirming fan as down, reconnect fan and confirm fan as up. Repeat this process for each fan that is monitored by the TSF.

Test 6 (power status):

Test 6a (conditional): If TOE employs redundant power supplies (PS), then test may be a simple matter of cycling one PS while leaving other power units untouched. Reset one PS while allowing the other(s) to remain up. Peruse system log and verify message indicating PS cycled (went down & up).

Test 6b (conditional): If TOE is supported by a single PS, than test has to be verified by waiting for system log to provide power status on periodic intervals. If system log does not report power status, then PS test failed.

### 2.2.1.2 Security Audit Review (FAU_SAR)

#### FAU_SAR.1/Log Audit Review (System Log)

*TSS*

There are no TSS EAs for this SFR.

*Operational Guidance*

There are no guidance EAs for this SFR.

*Test*

For each system log event described in FAU_GEN.1.1/Log, the evaluator shall review the system log to observe that they are displayed in real time. For those system log events that are periodic or persistent status messages, the evaluator shall observe that they are shown in the system log at the proper time. For those events that are triggered by a certain event, the evaluator shall cause that event to occur and ensure that it is logged. For example, the evaluator shall verify that the TOE logs data link connection status by unplugging and reconnecting the TOE's Ethernet connection and verifying that an appropriate log was generated for both. In all cases, the evaluator shall verify that the contents and formatting of the log data are consistent with what is defined in FAU_GEN.1.2/Log.

### 2.2.1.3 Security Audit Event Storage (FAU_STG)

#### FAU_STG.1/CDR Protected Audit Trail Storage (Call Detail Record)

*TSS*

The evaluator shall examine the TSS to ensure it describes how CDRs are protected against unauthorized modification or deletion. The evaluator shall also examine the TSS to ensure it describes any administrative access controls placed on CDR modification (e.g., Administrator Type 1 can modify/delete CDRs while Administrator Type 2 cannot modify/delete CDRs).

*Operational Guidance*

The evaluator shall examine the guidance documentation to determine that it describes any configuration required for protection of the locally stored CDRs against unauthorized modification. The evaluator shall also examine the documentation to ensure that any administrative access controls and configuration of the access controls on CDR access are described.

*Test*

The evaluator shall log in to the TOE as a Security Administrator and verify that authorized administrators are able to view stored CDRs but have no ability to modify them.

If an administrator access control restricts a user associated with the Security Administrator role from accessing CDR data, the evaluator shall then log in to the TOE as the user that lacks privilege to interact with CDRs and observe that there is no way for that user to access the CDR data.

### 2.2.1.4 Voice and Video Recording (FAU_VVR_EXT)

#### FAU_VVR_EXT.1 Recording Voice and Video Call Data

*TSS*

The evaluator shall examine the TSS to verify that it describes if the TSF has or does not have the capability to record voice and video call data.

*Operational Guidance*

There are no guidance EAs for this SFR.

*Test*

The test for this SFR is performed as part of FMT_SMF.1/ESC's EAs.

### 2.2.2 User Data Protection (FDP)

#### 2.2.2.1 Information Flow Control Policy (FDP_IFC)

##### FDP_IFC.1 Subset Information Flow Control

This SFR is tested in conjunction with FDP_IFF.1.

#### 2.2.2.2 Information Flow Control Functions (FDP_IFF)

##### FDP_IFF.1 Simple Security Attributes

*TSS*

The evaluator shall examine the TSS to verify that it describes the call control protocol(s) used by the TOE and the circumstances under which the TSF will transmit streaming media data. The evaluator shall verify that the TSF does not transmit any streaming media in circumstances where a VVoIP endpoint operator would not reasonably expect it to do so and whether there are any explicit overrides to the policy.

*Operational Guidance*

If any aspects of the TOE's call control functionality are configurable (such as the specific call control protocol used or the circumstances in which the TSF will or will not transmit streaming media data), the evaluator shall examine the operational guidance to verify that instructions for configuring this behavior are provided.

*Test*

The evaluator shall perform one or more of the following tests depending on the protocols that the TOE claims to support. For each test performed, the evaluator shall conduct the test for each supported environment (IPv4 and/or IPv6).

**If the TSF supports SIP:**

The evaluator shall set up a test environment where two SIP clients are registered to the TOE and the TSF is configured to allow call signals to capture through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from one SIP client to the other and observe via packet capture that two separate SIP connections are established: one from the caller to the TOE and the other from the TOE to the callee.

**If the TSF supports H.323:**

The evaluator shall set up a test environment where two H.323 clients are registered to the TOE and the TSF is configured to allow call signals to capture through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from one H.323 client to the other and observe via packet capture that two separate H.323 connections are established: one from the caller to the TOE and the other from the TOE to the callee.

**If the TSF supports SS7:**

Unlike H.323 & SIP which are call-setup and teardown protocols primarily used to process calls between local VVoIP endpoints that are registered to the ESC, the SS7 protocol focuses on setup and teardown of calls over the legacy Public Switch Telephone Network (PSTN). Therefore, when assessing the SS7 protocol, the evaluator will need to configure the TOE to make a call from a local VVoIP endpoint through its SS7 interface to a remote endpoint.

The evaluator shall set up a test environment where a single VVoIP endpoint is registered to the TOE (through H.323 or SIP) and the TSF is configured to allow call signals through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from the locally registered VVoIP endpoint to a remote endpoint that requires the use of the TOE's SS7 extension. The evaluator shall observe and capture SS7 signaling messages transiting through the TOE to both the local client and remote SS7-based endpoint. The evaluator shall verify that the TOE successfully sets up, processes, and tears down call between local VVoIP endpoint and external telephony device requiring SS7 signaling for connectivity. The evaluator shall also verify that the TOE transmits and receives the SS7 signaling messages IAM, ACM, and ANM to set up a call and RLC to tear down a call. The evaluator shall verify that SS7 call processing is employed by verifying that a two-way conversation can occur over the connected call.

If the TSF supports both H.323 and SIP, the evaluator shall repeat this test for the VVoIP endpoint registration method not chosen during the first iteration of the test.

**If the TSF supports MGCP:**

Unlike H.323 & SIP which are call-setup and teardown protocols primarily used to process calls between local VVoIP-clients that are registered to the ESC, the MGCP protocol focuses on the control of Media Gateways (MG) which set up voice calls between VVoIP networks and the PSTN. The TSF employs MGCP to control MGs that provision VVoIP calls for external connection to the PSTN and from the PSTN to the local VVoIP network. Therefore, when assessing the SS7 protocol, the evaluator will need to configure the TOE to make a call from a local VVoIP-client through its MGCP interface (i.e. MGC/Call Agent) to a remote endpoint.

The evaluator shall set up a test environment where a single VVoIP endpoint is registered to the TOE (through H.323 or SIP) and the TSF is configured to allow call signals through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from the locally registered VVoIP endpoint to a remote endpoint that requires the use of the TOE's MGCP extension for PSTN connection. The evaluator shall observe and capture MGCP signaling messages transiting the TOE to/from the local VVoIP endpoint and out to remote MGCP/PSTN endpoint. The evaluator shall verify that the TOE successfully sets up, processes, and tears down the call between the local VVoIP endpoint and external telephony device requiring MGC/PSTN signaling for connectivity. The evaluator shall also verify that the TOE transmits and receives the MGCP signaling messages NTFY, CRCX, and MDCX to set up a call and DLCX to tear down a call. The evaluator shall verify that MGCP call processing is employed by verifying that a two-way conversation can occur over the connected call.

If the TSF supports both H.323 and SIP, the evaluator shall repeat this test for the VVoIP endpoint registration method not chosen during the first iteration of the test.

### 2.2.2.3 Residual Information Protection (FDP_RIP)

#### FDP_RIP.1 Subset Residual Information Protection

*TSS*

The evaluator shall examine the TSS to ensure it describes the data objects overwritten as part of the sanitation operation. This should include both the TSF data that is overwritten as well as the characteristics of the physical drive that is erased (e.g. an entire drive, one or more logical partitions of a drive). The evaluator shall also examine the TSS to ensure that the sanitation process is described. In particular, the TSS must describe how the sanitation process follow the NIST 800-88 guidelines for "Disk Storage Sanitation."

*Operational Guidance*

The evaluator shall examine the guidance documentation to ensure it describes the data objects overwritten as part of the sanitation operation. The evaluation shall also ensure that the guidance documentation describes the administrative procedures necessary to trigger the sanitation operation. The evaluation shall also ensure that the TOE indication that the sanitization operation has completed is described, if applicable.

*Test*

The following test may require the evaluator to have access to developer tools.

The evaluator shall identify the storage locations (e.g. drives, disk partitions) that are erased when the TOE performs a wipe operation. The evaluator shall then populate each of these locations with large amounts of 'junk' data so that a known amount of their storage is used. The evaluator shall use the TOE to verify that the current storage levels are consistent with the amount of data that was introduced to each location.

The evaluator shall then initiate a wipe command and observe that each location that is subject to erasure is 100% free. The evaluator shall use forensic tools to examine each location that is subject to erasure and verify that the data has been overwritten by all zeroes.

### 2.2.3 Identification and Authentication (FIA)

#### 2.2.3.1 User Authentication (FIA_UAU)

##### FIA_UAU.2/TC User Authentication before Any Action (Telecommunications Devices)

*TSS*

The evaluator shall examine the TSS and ensure that the telecommunications device authentication procedures are described including a description of how the TOE prevents TSF-mediated actions by unauthenticated devices.

*Operational Guidance*

The evaluator shall examine the guidance documentation and ensure that any actions required to enable authentication of telecommunications devices is described.

*Test*

The following testing shall be repeated for each supported environment (IPv4 and/or IPv6):

The evaluator shall deploy the TOE in an environment with another ESC and configure both ESCs to support an encrypted trunk to one another, where the trunk is encrypted using a security protocol selected in FTP_ITC.1 from the Base-PP. The evaluator shall also deploy a packet sniffer on the encrypted trunk channel. The evaluator shall perform the following tests:

Test 1: The evaluator shall configure the TOE to accept encrypted trunk communications from the remote ESC using authentication credentials and IP address. The evaluator shall then use the remote ESC to connect to the TOE and verify that the encrypted trunk is successfully established. The evaluator shall use packet captures to verify that encrypted traffic is transmitted between the TOE and the remote ESC.

Test 2: The evaluator shall repeat test 1 but enter invalid credentials when attempting to authenticate. The evaluator shall observe that the encrypted trunk is not successfully established due to invalid credentials.

Test 3: The evaluator shall repeat test 1 but configure the TOE to accept encrypted trunk communications from a different IP address than what is assigned to the remote ESC. The evaluator shall then attempt to connect to the TOE using the remote ESC with valid credentials and observe that the encrypted trunk is not successfully established due to invalid IP address.

## FIA_UAU.2/VVoIP User Authentication before Any Action (VVoIP Endpoints)

*TSS*

The evaluator shall examine the TSS and ensure that the VVoIP endpoint authentication procedures are described including a description of how the TOE prevents TSF-mediated actions by unauthenticated devices. In addition to establishment of voice/video calls, this includes TOE-initiated application of an update to the VVoIP endpoint software/firmware.

*Operational Guidance*

The evaluator shall examine the guidance documentation and ensure that any actions required to authenticate VVoIP endpoints are described.

*Test*

The following testing shall be repeated for each supported environment (IPv4 and/or IPv6):

The evaluator shall ensure that the TSF is configured to support encrypted SIP and/or H.323 client connections and that any VVoIP endpoint devices used for this testing can use the protocol that the TSF is configured to support.

The evaluator shall perform the following tests:

Test 1: The evaluator shall attempt to place a call with a VVoIP endpoint device without registering to the TOE. The attempt should fail. The evaluator shall also attempt to download an update from the TOE and observe failure.

Test 2 [Conditional on TOE requiring certificate authentication to establish the connection used for registration]: The evaluator shall load an invalid certificate onto a VVoIP endpoint device and initiate the registration process. The registration process should fail due to an invalid certificate.

Test 3: The evaluator shall connect to the TOE and initiate the registration process. When prompted for credentials, the evaluator shall supply invalid credentials and observe that the registration process fails for that reason.

Test 4: The evaluator shall connect to the TOE and initiate the registration process. When prompted for credentials, the evaluator shall supply valid credentials and observe that the registration process succeeds and that the registered device can be used to place calls.

### 2.2.4 Security Management (FMT)

#### 2.2.4.1 Secure by Default Configuration (FMT_CFG_EXT)

##### FMT_CFG_EXT.1 Secure by Default Configuration

*TSS*

The evaluator shall check the TSS and ensure that it identifies if the TOE is delivered with default or no Security Administrative credentials. The evaluator shall also check the TSS and ensure that the functionality available when the TOE is configured with default credentials or no credentials is identified. The evaluator shall examine the identified functionality and ensure that only enough functionality to set new Security Administrator credentials is available when the TOE is configured with default credentials or no credentials.

*Operational Guidance*

The evaluator shall check the guidance documentation and ensure that the administrative functionality that is available when the TOE is configured with default credentials or no credentials is identified. The evaluator shall examine the guidance documentation and ensure the instructions for establishing new Security Administrative credentials is described.

*Test*

Note that this test may only be deployed the first time the TOE is run or immediately following a factory reset.

The evaluator shall perform the initial setup steps for the TOE as specified in the administrative guidance. The evaluator shall verify that if a default administrative account is used to log in to the TOE for the first time, the login event is immediately followed by a prompt to change the password for the default account. If no default account is used, the evaluator shall verify that they are prompted to define an initial administrator account and that no further security-relevant actions can be performed until the evaluator has authenticated to the TOE using that account.

#### 2.2.4.2 Specification of Management Functions (FMT_SMF)

##### FMT_SMF.1/ESC Specification of Management Functions (ESC)

*TSS*

For each management function specified in FMT_SMF.1.1/ESC, the evaluator shall conform that the management function is provided by the TOE. The evaluator shall also conform that the TSS details, for each supported management interface, which specific functions are available at that interface.

*Operational Guidance*

If "Ability to enable/disable voice and video recordings for any registered VVoIP endpoint" is selected, the evaluator shall examine the guidance document to verify it describes how to enable or disable recordings of voice and video calls.

*Test*

Test 1 (Conditional): If “Ability to enable/disable voice and video recordings for any registered VVoIP endpoint” is selected, the evaluator shall deploy a test environment with two or more registered VVoIP endpoints. The evaluator shall choose two endpoints and configure the TOE to ~~disable~~ enable voice/video recording between them. The evaluator shall place a call between the two selected endpoints, verify that the call is successfully established, then terminate the call and verify that a recording is generated. The evaluator shall then configure the TOE to disable voice/video recording between the same two endpoints, repeat the call, verify that the call is established, then terminate the call. The evaluator shall examine the location where the first recording was generated and verify that no new recording is generated.

Test 2: The evaluator shall deploy a test environment with two or more registered VVoIP endpoints. The evaluator shall choose two endpoints, place a call between them, and verify that the call is successfully established. While the call is active, the evaluator shall use the TSF to review active connections and verify that the VVoIP endpoints' connections to the TOE are active. The evaluator shall discontinue the call and verify that the TSF no longer shows the VVoIP endpoints' connections to the TOE as active.

Test 3 (Conditional): If "ability to configure the password policy" is selected, the evaluator shall observe what the password strength policy is configured to by default on the TOE and shall verify that it is enforced by defining several weak administrative passwords for a given administrator account that are appropriately rejected by the TSF. The evaluator shall then modify the TOE's password policy in such a manner that at least one of these weak passwords would now be accepted by the policy. The evaluator shall repeat the attempted password changes and observe that the TSF correctly accepts or rejects the passwords based on the new policy.

## 2.2.5 Protection of the TSF (FPT)

### 2.2.5.1 Fail Secure (FPT_FLS)

#### FPT_FLS.1 Failure with Preservation of a Secure State

*TSS*

The evaluator shall examine the TSS to verify that it describes the TOE failures that can occur and the TOE's response to these failures. The evaluator shall also examine the TSS to verify that it provides sufficient detail to justify how the TOE's responses to these failures preserves a secure state.

*Operational Guidance*

The evaluator shall examine the guidance documentation and ensure that if the TOE's failure handling behavior is configurable, any instructions for doing so are provided. The evaluator shall also examine the guidance documentation to verify that it identifies the potential failures that can occur and the TOE's response to them so that the reader is aware of when the TSF has failed to a secure state.

*Test*

The evaluator shall perform the EAs for FPT_TST_EXT.1 as defined in the NDcPP SD. For each self-test failure, the evaluator shall verify that the observed TOE behavior is consistent with the failure state defined in the TSS for this SFR. If this functionality is configurable, the evaluator shall reconfigure the TOE to each possible response to a self-test failure and re-execute the testing as many times as is necessary to demonstrate that the configured behavior is observed in each case.

### 2.2.6 Trusted Path/Channels (FTP)

#### 2.2.6.1 Inter-TSF Trusted Channel (FTP_ITC)

#### FTP_ITC.1/ESC Inter-TSF Trusted Channel (ESC Communications)

*TSS*

The evaluator shall perform the TSS evaluation activities specified in the NDcPP SD for FTP_ITC.1 for the communications interfaces and protocols specified in this iteration of the requirement.

*Operational Guidance*

The evaluator shall perform the AGD evaluation activities specified in the NDcPP SD for FTP_ITC.1 for the communications interfaces and protocols specified in this iteration of the requirement.

*Test*

In addition to the assurance activities specified in the NDcPP SD for FTP_ITC.1, the evaluator shall perform the following tests:

Test 1: For each combination of signaling protocol (SIP, H.323), method of securing that protocol (IPsec, TLS), and method of securing transmitted media (SRTP, DTLS), the evaluator shall configure the TOE to use the selected protocols through a trunk to a remote ESC. The evaluator shall register a VVoIP endpoint to the TOE and a second VVoIP endpoint to the remote ESC. The evaluator shall place a packet sniffer on the network and capture traffic from the TOE to the local VVoIP endpoint and the remote ESC. The evaluator shall then place a call from one VVoIP endpoint to the other. The evaluator shall verify that the TOE's audit trail shows that the local VVoIP endpoint was configured as a client using the configured protocol, that the traffic between the local VVoIP endpoint and the TOE is unintelligible, and that the traffic between the TOE and the remote ESC is protected for both signaling and media communications using the configured methods of securing them.

The evaluator shall repeat this test as many times as is necessary to demonstrate that each combination of securing the signaling protocol communications, securing the media protocol communications, and securing the SIP trunk from the TOE to the remote ESC can be used as claimed. Note that in any case where this results in double encryption of the traffic (e.g. SRTP-protected media tunneled through IPsec over a SIP trunk), the evaluator shall conduct the test with the outer layer enabled and then disabled in order to verify that both methods of protection are being used.

Test 2 (conditional): If 'VVoIP conferencing system' is selected, the evaluator shall repeat test 1 (depending on the protocols the TOE claims to support) in an environment where the TOE is being used to establish a conference call between three or more registered VVoIP endpoints. In both cases, the evaluator shall verify that all SIP and SRTP traffic is encrypted.

# 3 Evaluation Activities for Optional Requirements

## 3.1 Protection of the TSF (FPT)

### 3.1.1 Trusted Update (FPT_TUD_EXT)

#### FPT_TUD_EXT.1/VVoIP Trusted Update (VVoIP Endpoints)

*TSS*

The evaluator shall examine the TSS to verify that it describes the ability of the TOE to retrieve VVoIP endpoint software/firmware updates and the process by which VVoIP endpoints can register to the TOE and acquire these updates. The evaluator shall also examine the TSS to verify that it describes by which the authenticity and integrity of VVoIP endpoint software updates are assured and what role the TSF has in ensuring that updates are genuine.

*Operational Guidance*

The evaluator shall examine the operational guidance to verify that it provides instructions on how to acquire and verify a VVoIP endpoint software/firmware update from the manufacturer. The evaluator shall also verify that the guidance includes instructions on how an ESC administrator can use the TOE to apply software/firmware updates to registered VVoIP endpoints.

*Test*

The evaluator shall perform the following test:

Step 1: Prior to downloading software update from TOE to registered VVoIP-client, the evaluator shall check to ensure the current version of the registered client device can be appropriately obtained by means of the operation methods specified by the administrator guidance.

Step 2: The evaluator shall check to ensure that VVoIP endpoint software/firmware updates are signed and/or hashed by the manufacturer based on what is specified in the ST.

Step 3: The evaluator shall check to ensure that only administrators of the TOE are permitted to initiate an update to a registered VVoIP endpoint.

Step 4: The evaluator shall check to ensure that software updates are correctly performed by verifying that the VVoIP endpoint is running the newly-obtained software version obtaining the newly updated software version of the VVoIP-client device once update has complete.

Note: In some cases the ESC will not receive an explicit message from the VVoIP endpoint stating that the software update executed successfully. In addition, some software updates will not take effect until a reboot of the VVoIP endpoint is initiated remotely by the ESC or manually/physically at the VVoIP endpoint device itself. In either scenario, the VVoIP endpoint itself will always indicate whether verification of the update has failed. Therefore, the tester can (or may have to) verify successful software download by querying the VVoIP endpoint device for new software/firmware version. The tester can also verify whether software update failed by querying the registered VVoIP endpoint for errors.

In most cases, failed software update messages will originate from the VVoIP endpoint and not the ESC. Any failed software update reported by the registered VVoIP endpoint should have the report forwarded to the TOE. However, as mentioned earlier, the registered VVoIP endpoint may not report successful software downloads an therefore no 'successful download' report should be expected to be forwarded to the ESC. If the VVoIP endpoint does report a ‘software download complete’ or just ‘complete’, then the TOE should receive a message indicating that the download was completed. When the VVoIP endpoint reboots, it is expected to report the new software/firmware version to the TOE so that the new version will be displayed in the OA&M application.

Step 5: The evaluator shall check to ensure that the verification of software/firmware updates from the TOE to the VVoIP endpoint fails using unauthorized data or improperly signed updates. The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.

Note: this may require the evaluator to obtain a deliberately invalid software update from the device manufacturer or developer access to the TOE so that a stored update can be manipulated directly in a manner that will cause signature and/or hash verification to fail.

# 4 Evaluation Activities for Selection-Based Requirements

## 4.1 Security Audit (FAU)

### 4.1.1 Security Audit Event Selection (FAU_SEL)

#### 4.1.1.1 FAU_SEL.1 Selective Audit

*TSS*

The evaluator shall examine the TSS to verify that it identifies the attributes by which the TOE can be configured to selectively enable or disable the generation of auditable events.

*Operational Guidance*

The evaluator shall examine the operational guidance to verify that it provides a list of the attributes that can be used to selectively enable or disable the generation of auditable events as well as instructions for performing this operation.

*Test*

Note that the following testing may be done in conjunction with other EAs since auditable events occur as a by-product of the TOE being used to perform other security functions.

The evaluator shall perform TSF-mediated actions with all auditable events enabled and observe that these events are audited as expected. The evaluator shall then log on to the TOE and disable auditable events by each attribute defined in the ST. The evaluator shall then re-execute the same set of TSF-mediated actions as before and observe that audit logs are not generated for all auditable events that are administratively disabled.

### 4.1.2 Security Audit Event Storage (FAU_STG)

#### 4.1.2.1 FAU_STG.1/VVR Protected Audit Trail Storage (Voice/Video Recording)

*TSS*

The evaluator shall examine the TSS to verify that it describes the method by which locally-stored voice and video recordings are protected and that this method uses cryptographic mechanisms defined in FCS_COP.1.

*Operational Guidance*

If the TOE provides the ability to enable/disable encryption of locally stored voice and video recordings, the evaluator shall verify that the operational guidance provides instructions on how to enable encryption and directs the reader to ensure that this is enabled in the TOE's evaluated configuration.

*Test*

The evaluator shall perform the following tests:

Test 1: The evaluator shall verify that the TSF provides no interface to access voice/video recording data stored on the TOE except for legitimate access from an authorized administrator through the Operations, Administration, and Management (OA&M) interface.

Test 2: Both B2B subscriber calls and voice/video conferencing calls may be stored on the TOE based on safeguards (i.e. secured or unsecured) for which they were recorded. The evaluator shall identify the location of stored voice and video records and verify that this data is stored in an encrypted format for all types of voice and video calls that can be processed by the TOE. If this functionality is configurable, the evaluator shall follow the operational guidance to enable encryption prior to generating any voice/video recordings.

### 4.1.3 Voice and Video Recording (FAU_VVR_EXT)

#### 4.1.3.1 FAU_VVR_EXT.2 Generation of Voice and Video Recordings

*TSS*

The evaluator shall examine the TSS to ensure that it describes the conditions that can be set for the retention of voice/video recordings (all calls to/from a specific endpoint are recorded by administrator control, user manually specifies a call to be recorded at the start of the call session, etc.) and that these are consistent with what is specified in FAU_VVR_EXT.2.1. The evaluator shall also ensure that the TSS describes how voice/video recordings are retained, both in terms of the supported audio/video formats and how each recording is uniquely identified for future access.

*Operational Guidance*

The evaluator shall examine the operational guidance to ensure that it describes how retention for voice/video recordings can be enabled and disabled, how stored records are encoded, and how they are uniquely identified.

*Test*

The evaluator shall disable all mechanisms for voice/video recording. The evaluator shall then place a call that is mediated by the TSF and observe that no recording is generated after the call is completed. The evaluator shall then configure the TSF to enable recording, repeat the call, and ensure that a recording is generated in the required format after the call is completed. The evaluator shall then repeat this process and observe that a second recording is generated, and that the two recordings can be distinguished from one another using unique identifying information. The evaluator shall then disable recording, repeat the call, and observe that a recording is not generated.

If the TSF supports multiple mechanisms for enabling the recording of voice/video data, the evaluator shall repeat this test for each supported mechanism to ensure that voice/video recordings are only generated when that mechanism is active.

# 5 Evaluation Activities for SARs

To evaluate the SARs specified by the Base-PP and this PP-Module, the evaluator shall perform the SAR EAs defined in Base-PP against the entire TOE as applicable.

## 5.1 Class AVA: Vulnerability Assessment

An ESC TOE is often represented as a software application that is installed onto a general-purpose server which is operated as a dedicated ESC device. In order to ensure that the OE.NO_GENERAL_PURPOSE environmental objective is satisfied, the evaluator shall conduct vulnerability research and penetration testing related to privilege escalation in order to attempt to 'break out' of the ESC interface provided by the administrator and gain general-purpose administrative functionality over the underlying OS. If the evaluator is able to use the underlying OS to affect the behavior of the TOE (through the ability to use general-purpose CLI commands or perform functions via a GUI) or introduce an application or service that causes the network device to be listening on a Transmission Control Protocol TCP or User Datagram Protocol port, the vulnerability testing will result in failure. Note that it is acceptable for administrators to have read-only access to certain areas of the OS file system if this behavior is intended by the TOE developer; only write and execute access are prohibited.

# 6 Required Supplementary Information

This SD has no required supplementary information beyond the TSS, operational guidance, and testing.

# 7 References

*Table 3: References*

| Identifier | Title |
|---|---|
| **[CC]** | Common Criteria for Information Technology Security Evaluation –<br>• Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017<br>• Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017<br>• Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 |
| **[CEM]** | Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017 |
| **[NDcPP]** | Collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 |
| **[NDcPP SD]** | Supporting Document – Mandatory Technical Document – Evaluation Activities for Network Device cPP, Version 2.2, December 2019 |
| **[NIST SP 800-88]** | Guidelines for Media Sanitization, Revision 1, December 2014 |
| **[ESC]** | PP-Module for Enterprise Session Controller (ESC), Version 1.0, November 19, 2020 |