ONVIF Profile C Client Test Specification

Version 16.01 January, 2016

Table of Contents

Introduction

The goal of the ONVIF Test Specification set is to make it possible to realize fully interoperable IP physical security implementations from different vendors. This specification also acts as an input document to the development of a test tool which will be used to test the ONVIF Client implementation conformance towards ONVIF standard. This Client Test Tool analyzes network communications between ONVIF Devices and Clients being tested and determines whether a specific Client is ONVIF conformant (see ONVIF Conformance Process Specification).

This particular document defines test cases required for testing Profile C features of a Client application e.g. System Component Information, System Component State, Door Control and Access Point Control. It also describes the test framework, test setup, prerequisites, test policies needed for the execution of the described test cases.

Scope

This ONVIF Profile C Client Test Specification defines and regulates the conformance testing procedure for the ONVIF conformant Clients in the scope of Profile C features. Conformance testing is meant to be black-box network traces analysis and verification. The objective of this specification is to provide the test cases to test individual requirements of ONVIF Clients in the scope of Profile C features according to ONVIF Profile Specifications.

The principal intended purposes are:

- Provide self-assessment tool for implementations.
- Provide comprehensive test suite coverage for Profile C features.

This specification **does not** address the following:

- 3rd parties Client use cases
- Non-functional (performance and regression) testing and analysis.
- SOAP Implementation Interoperability test i.e. Web Services Interoperability Basic Profile version 2.0 (WS-I BP2.0).
- Network protocol implementation Conformance test for HTTPS and HTTP protocols.

The following sections cover test cases needed for the verification of relevant features as mentioned in the ONVIF Profile Specifications.

System Component Information

System Component Information section specifies Client ability to request lists of Access Points, Doors and Areas from Device.

System Component State

System Component State section specifies Client ability to request information about the state of Access Points (enabled/disabled) and Doors (locked, unlocked, etc.).

Door Control

Door Control section specifies Client ability to to control Doors (access door, lock door, unlock door, etc.).

Access Point Control

Access Point Control section specifies Client ability to control Access Points (enabled/disabled).

External Authorization

External Authorization section specifies Client ability to receive authorization request from Device and then make decisions about granting access and send it to Device. This section also specifies Client ability to retrieve and receive notifications about access decisions related to External Authorization.

Access Control Decisions

Access Control Decisions section specifies Client ability to receive notifications about access decisions related to Access Control.

Configuration Change Notifications

Configuration Change Notifications section specifies Client ability to receive notifications about access points, doors, and areas configuration change.

Duress Notifications

Duress Notifications section specifies Client ability to receive notifications about duress situation.

Normative references

ONVIF Conformance Process Specification:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Profile Policy:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Core Specifications:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Core Client Test Specification:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Profile A Specification:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Access Rules Specification:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Credential Specification:

http://www.onvif.org/Documents/Specifications.aspx

ONVIF Schedule Specification:

http://www.onvif.org/Documents/Specifications.aspx

ISO/IEC Directives, Part 2:

http://www.iso.org/directives

ISO 16484-5:2014-09 Annex P:

https://www.iso.org/obp/ui/#!iso:std:63753:en

Rules for the structure and drafting of International Standards, Annex H: Verbal forms for the expression of provisions.

Terms and Definitions

Conventions

The key words "shall", "shall not", "should", "should not", "may", "need not", "can", "cannot" in this specification are to be interpreted as described in [ISO/IEC Directives Part 2].

Definitions

This section describes terms and definitions used in this document.

Profile See ONVIF Profile Policy.

Profile C The Profile C Specification.

ONVIF Device	Computer appliance or software program that exposes one or multiple ONVIF Web Services.
ONVIF Client	Computer appliance or software program that uses ONVIF Web Services.
Conversation	A Conversation is all exchanges between two MAC addresses that contains SOAP request and response.
Network	A network is an interconnected group of devices communicating using the Internet protocol.
Network Trace Capture file	Data file created by a network protocol analyzer software (such as Wireshark). Contains network packets data recorded during a live network communications.
SOAP	SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols.
Client Test Tool	ONVIF Client Test Tool that tests ONVIF Client implementation towards the ONVIF Test Specification set.

Door	A physical door, barrier, turnstile, etc which can be controlled remotely and restricts access between two areas. A door is usually equipped with an electronic lock and a sensor.
Door Alarm	An abnormal state of the door where door is forced open or held open beyond the permitted time duration.
Door Mode	Logical state of the door indicating whether the door is locked, unlocked, blocked, locked down or locked open etc.
Lock	An operation after which a door is locked and alarm is unmasked.
Unlock	An operation to allow a door to be freely used for passage without any door alarms being triggered.
Access Point	A logical composition of a physical door and ID point(s) controlling access in one direction.
Disable Access Point	If an Access Point is disabled, it will not be considered in the decision making process and no commands will be issued from that Access Point to the Door configured for that Access Point. When an Access Point is disabled, the associated ID Point may or may not be disabled or shut down. Clients may still be able to command the Door Controller to control associated door even though that door is also referenced by a disabled access point.
ID Point	A device that converts reader signals to protocols recognized by an authorization engine. It can be card reader, REX, biometric reader etc.
Valid Device Response	Device has responded to specific request with code HTTP or RTSP 200 OK and SOAP fault message has not appeared.

Abbreviations

This section describes abbreviations used in this document.

PACS	Physical Access Control System.
tns1:	A prefix for the ONVIF topic namespace "http://www.onvif.org/ver10/topics". This prefix is not part of the standard and an implementation can use any prefix. See Core Specification description of Namespaces for details.
HTTP	Hyper Text Transport Protocol.
HTTPS	Hyper Text Transport Protocol over Secure Socket Layer.
URI	Uniform Resource Identifier.
WSDL	Web Services Description Language.
XML	eXtensible Markup Language.

Namespaces

Prefix and namespaces used in this test specification are listed in Table 1. These prefixes are not part of the standard and an implementation can use any prefix.

Table 1. Defined namespaces in this specification

Prefix	Namespace URI	Description
soapenv	http://www.w3.org/2003/05/soap-envelope	Envelope namespace as defined by SOAP 1.2 [SOAP 1.2, Part 1]
xs	http://www.w3.org/2001/XMLSchema	Instance namespace as defined by XS [XML-Schema, Part1] and [XMLSchema,Part 2]
xsi	http://www.w3.org/2001/XMLSchema-instance	XML schema instance namespace
tns1	http://www.onvif.org/ver10/topics	The namespace for the ONVIF topic namespace
tt	http://www.onvif.org/ver10/schema	ONVIF XML schema descriptions
tev	http://www.onvif.org/ver10/events/wsdl	The namespace for the WSDL event service
tac	http://www.onvif.org/ver10/accesscontrol/wsdl	The namespace for the WSDL access control service
tdc	http://www.onvif.org/ver10/doorcontrol/wsdl	The namespace for the WSDL door control service

Test Overview

This section provides information for the test setup procedure and required prerequisites that should be followed during test case execution.

An ONVIF Client conformant to Profile C is an ONVIF Client that can request information regarding the Physical Access Control System (PACS) related entities from an ONVIF Device conformant to Profile C and do basic control of Doors and Access Points over an IP network. ONVIF Client can also retrieve and receive standardized PACS related events.

An ONVIF Profile is described by a fixed set of functionalities through a number of services that are provided by the ONVIF standard. A number of services and functionalities are mandatory for each type of ONVIF Profile. An ONVIF Device and ONVIF Client may support any combination of Profiles and other optional services and functionalities.

General

Test Cases are grouped depending on features. Each Test Cases group provides description of feature requirement level for Profiles, expected scenario under test and related test cases:

- Feature Level Requirement
- Expected Scenarios Under Test
- List of Test Cases

Feature Level Requirement

Feature Level Requirement item contains a feature ID and feature requirement level for the Profiles, which will be used for Profiles conformance.

If Feature Level Requirement is defined as Mandatory for some Profile, Client shall pass Expected Scenario Under Test for each Device with this Profile support to claim this Profile Conformance.

If Feature Level Requirement is defined as Conditional, Optional for some Profile, Client shall pass Expected Scenario Under Test for at least one Device with this Profile support to claim feature as supported.

Expected Scenarios Under Test

Expected Scenarios Under Test item contains expected scenario under test, conditions when the feature will be defined as supported and as not supported.

Test Cases

Test Case items contain list of test cases which are related to feature. Test cases provide exact procedure of testing feature support conditions.

Each Test Case contains the following parts:

- Test Label - Unique label for each test
- Test Case ID - Unique ID for each test
- Profile Normative References - Requirement level for the feature under test is defined in Profile Specification. This reference is informative and will not be used in conformance procedure.
- Feature Under Test - Feature which is under current test. Typically a particular command or an event.
- Test Purpose - The purpose of current test case.
- Pre-Requisite - The pre-requisite defines when the test should be performed. In case if pre-reqiusite does not match, the test result will be NOT DETECTED.
- Test Procedure - scenario expected to be reflected in network trace file.
- Test Result - Passed and failed criteria of the test case. Depending on these criteria test result will be defined as PASSED or FAILED.
- Validated Feature List - list of features ID related to this test case.

Test Setup

Collect Network Traces files required by the test cases.

Collect Feature List XML files for Devices detected in the Network Trace files.

Client shall support all mandatory and conditional features listed in the Device Feature List XML file supplied for the Profiles supported by the Client.

For compatibility with the Profile C, the ONVIF Client shall follow the requirements of the conformance process. For details please see the latest ONVIF Conformance Process Specification.

Prerequisites

The pre-requisites for executing the test cases described in this Test Specification include:

The Device shall be configured with an IPv4 address.

The Device shall be able to be discovered by the Client.

System Component Information Test Cases

Expected Scenarios Under Test:

1. Client connects to Device to retrieve a lists of Access Points, Doors and Areas.
2. Client is considered as supporting System Component Information if the following conditions are met:
    - Client is able to list available Access Points using GetAccessPointInfoList operation AND
    - Client is able to list available Doors using GetDoorInfoList operation AND
    - Client is able to list available Areas using GetAreaInfoList operation.
3. Client is considered as NOT supporting System Component Information if ANY of the following is TRUE:
    - No valid responses for GetAccessPointInfoList OR
    - No valid responses for GetDoorInfoList OR
    - No valid responses for GetAreaInfoList.

LISTING OF ACCESS POINTS

Test Label: System Component Information - Listing of Access Points

Test Case ID: SYSTEMCOMPONENTINFORMATION-1

Profile C Requirement: Mandatory

Feature Under Test: System Component Information

Test Purpose: To verify that list of all access points items provided by Device is received by Client using the GetAccessPointInfoList operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with GetAccessPointInfoList operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes GetAccessPointInfoList request message to retrieve complete list of all access points configured on the Device.
2. Device responses with code HTTP 200 OK and GetAccessPointInfoListResponse message.

Test Result:

PASS -

- Client GetAccessPointInfoList request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client GetAccessPointInfoList request message has a proper hierarchy (refer to accesscontrol.wsdl) AND

- [S1] Client request contains "<GetAccessPointInfoList>" tag after the "<Body>" tag AND
- [S2] Device response contains "HTTP/* 200 OK" AND
- [S3] Device response contains "<GetAccessPointInfoListResponse>" tag AND
- [S4] At least one Device response in the same Conversation does not contain: "<NextStartReference>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: SystemComponentInformation_AccessPointInfoList

LISTING OF DOORS

Test Label: System Component Information - Listing of Doors

Test Case ID: SYSTEMCOMPONENTINFORMATION-2

Profile C Requirement: Mandatory

Feature Under Test: System Component Information

Test Purpose: To verify that list of all doors items provided by Device is received by Client using the GetDoorInfoList operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with GetDoorInfoList operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes GetDoorInfoList request message to retrieve complete list of all doors configured on the Device.
2. Device responses with code HTTP 200 OK and GetDoorInfoListResponse message.

Test Result:

PASS -

- Client GetDoorInfoList request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client GetDoorInfoList request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<GetDoorInfoList>" tag after the "<Body>" tag AND
  - [S2] Device response contains "HTTP/* 200 OK" AND
  - [S3] Device response contains "<GetDoorInfoListResponse>" tag AND
  - [S4] At least one Device response in the same Conversation does not contain: "<NextStartReference>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: SystemComponentInformation_DoorInfoList

LISTING OF AREAS

Test Label: System Component Information - Listing of Areas

Test Case ID: SYSTEMCOMPONENTINFORMATION-3

Profile C Requirement: Mandatory

Feature Under Test: System Component Information

Test Purpose: To verify that list of all areas items provided by Device is received by Client using the GetAreaInfoList operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with GetAreaInfoList operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes GetAreaInfoList request message to retrieve complete list of all areas configured on the Device.
2. Device responses with code HTTP 200 OK and GetAreaInfoListResponse message.

Test Result:

PASS -

- Client GetAreaInfoList request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client GetAreaInfoList request message has a proper hierarchy (refer to accesscontrol.wsdl) AND
  - [S1] Client request contains "<GetAreaInfoList>" tag after the "<Body>" tag AND
  - [S2] Device response contains "HTTP/* 200 OK" AND
  - [S3] Device response contains "<GetAreaInfoListResponse>" tag AND
  - [S4] At least one Device response in the same Conversation does not contain: "<NextStartReference>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: SystemComponentInformation_AreaInfoList

System Component State Test Cases

Expected Scenarios Under Test:

1. Client invokes a specific System Component State command to retrieve current state of Device in the system.

2. Client uses Pull Point event mechanism to receive Device state updates.

3. Client is considered as supporting System Component State if the following conditions are met:

   - Client is able to receive a state of access point through the use of Pull Point event mechanism AND

   - Client is able to receive a state of door through the use of Pull Point event mechanism

4. Client is considered as NOT supporting System Component State if ANY of the following is TRUE:

   - Client unable to receive Pull Point event message with a state of access point OR

   - Client unable to receive Pull Point event message with a state of door OR

STATE OF ACCESS POINTS

Test Label: System Component State - State of Access Points

Test Case ID: SYSTEMCOMPONENTSTATE-1

Profile C Requirement: Mandatory

Feature Under Test: System Component State

Test Purpose: To verify that Client is able to receive state of access point through the use of Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with CreatePullPointSubscription, PullMessages operations present.

- SYSTEMCOMPONENTINFORMATION-1 has passed.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message without any filter or with appropriate filter.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

3. Client invokes PullMessages command with Timeout and MessageLimit elements.

4. Device responses with code HTTP 200 OK and PullMessagesResponse message.

Test Result:

NOTE: In case when Filter is specified for Client **CreatePullPointSubscription** request message and if it does not contain "*:AccessPoint/State" OR "*:AccessPoint//." value of "<TopicExpression>" tag then Test shall be deemed as "NOT DETECTED".

PASS -

- Client **CreatePullPointSubscription** request message is a well-formed SOAP request (refer to onvif.xsd) AND

- Client **CreatePullPointSubscription** request message has a proper hierarchy (refer to event.wsdl) AND

  - [S1] Client request contains "<CreatePullPointSubscription>" tag after the "<Body>" tag AND

- [S2] (Client request does not contain "<Filter>" tag OR
- ([S2] "<CreatePullPointSubscription>" includes tag: "<Filter>" AND "<Filter>" includes tag: "<TopicExpression>" AND "<TopicExpression>" contains value EITHER ("*:AccessPoint/State" OR ":AccessPoint//."))) AND
- [S3] Device response contains "HTTP/* 200 OK" AND
- [S4] Device response contains "<CreatePullPointSubscriptionResponse>" tag AND

- Client PullMessages request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client PullMessages request message has a proper hierarchy (refer to event.wsdl) AND
  - [S5] Client request contains "<PullMessages>" tag after the "<Body>" tag AND
  - [S6] "<PullMessages>" includes tag: "<Timeout>" AND
  - [S7] "<PullMessages>" includes tag: "<MessageLimit>" AND
  - [S8] Device response contains "HTTP/* 200 OK" AND
  - [S9] Device response contains "<PullMessagesResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: SystemComponentState_AccessPointState

STATE OF DOORS

Test Label: System Component State - State of Doors

Test Case ID: SYSTEMCOMPONENTSTATE-2

Profile C Requirement: Mandatory

Feature Under Test: System Component State

Test Purpose: To verify that Client is able to receive state of door through the use of Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with CreatePullPointSubscription, PullMessages operations present.
- SYSTEMCOMPONENTINFORMATION-2 has passed.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message without any filter or with appropriate filter.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.
3. Client invokes PullMessages command with Timeout and MessageLimit elements.

4. Device responses with code HTTP 200 OK and PullMessagesResponse message.

Test Result:

NOTE: In case when Filter is specified for Client **CreatePullPointSubscription** request message and if it does not contain "*:Door/State" OR "*:Door//." value of "<TopicExpression>" tag then Test shall be deemed as "NOT DETECTED".

PASS -

- Client **CreatePullPointSubscription** request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client **CreatePullPointSubscription** request message has a proper hierarchy (refer to event.wsdl) AND
  - [S1] Client request contains "<CreatePullPointSubscription>" tag after the "<Body>" tag AND
  - [S2] (Client request does not contain "<Filter>" tag OR
  - ([S2] "<CreatePullPointSubscription>" includes tag: "<Filter>" AND "<Filter>" includes tag: "<TopicExpression>" AND "<TopicExpression>" contains value EITHER ("*:Door/State" OR "*:Door//."))) AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<CreatePullPointSubscriptionResponse>" tag AND
- Client PullMessages request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client PullMessages request message has a proper hierarchy (refer to event.wsdl) AND
  - [S5] Client request contains "<PullMessages>" tag after the "<Body>" tag AND
  - [S6] "<PullMessages>" includes tag: "<Timeout>" AND
  - [S7] "<PullMessages>" includes tag: "<MessageLimit>" AND
  - [S8] Device response contains "HTTP/* 200 OK" AND
  - [S9] Device response contains "<PullMessagesResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: SystemComponentState_DoorState

Door Control Test Cases

Expected Scenarios Under Test:

1. Client invokes a specific, valid mandatory Door Control command in order to change the state of door.
2. Client is considered as supporting Door Control if the following conditions are met:
   - Device returns a valid response to AccessDoor request AND

- Device returns a valid response to LockDoor request AND
- Device returns a valid response to UnlockDoor request
- When Device and Client support any of the following conditional features:
  - Device returns a valid response to DoubleLockDoor request OR
  - Device returns a valid response to BlockDoor request
- When Device and Client support LockDown conditional features:
  - Device returns a valid response to LockDownDoor request AND
  - Device returns a valid response to LockDownReleaseDoor request
- When Device and Client support LockOpen conditional features:
  - Device returns a valid response to LockOpenDoor request AND
  - Device returns a valid response to LockOpenReleaseDoor request.

3. Client is considered as NOT supporting Door Control if ANY of the following is TRUE:

- No valid Device response to AccessDoor request OR
- No valid Device response to LockDoor request OR
- No valid Device response to UnlockDoor request
- When Device and Client support any of the following conditional features:
  - No valid Device response to DoubleLockDoor request AND
  - No valid Device response to BlockDoor request
- When Device and Client support LockDown conditional features:
  - No valid Device response to LockDownDoor request OR
  - No valid Device response to LockDownReleaseDoor request
- When Device and Client support LockOpen conditional features:
  - No valid Device response to LockOpenDoor request OR
  - No valid Device response to LockOpenReleaseDoor request.

ACCESS DOOR OPERATION

Test Label: Door Control - AccessDoor

Test Case ID: DOORCONTROL-1

Profile C Requirement: Mandatory

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of door using AccessDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with AccessDoor operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes AccessDoor request message to change the state of door.
2. Device responses with code HTTP 200 OK and AccessDoorResponse message.

Test Result:

PASS -

- Client AccessDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client AccessDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<AccessDoor>" tag after the "<Body>" tag AND
  - [S2] "<AccessDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<AccessDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_AccessDoor

LOCK DOOR OPERATION

Test Label: Door Control - LockDoor

Test Case ID: DOORCONTROL-2

Profile C Requirement: Mandatory

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of door using LockDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with LockDoor operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes LockDoor request message to change the state of door.
2. Device responses with code HTTP 200 OK and LockDoorResponse message.

Test Result:

PASS -

- Client LockDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client LockDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<LockDoor>" tag after the "<Body>" tag AND
  - [S2] "<LockDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<LockDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_LockDoor

UNLOCK DOOR OPERATION

Test Label: Door Control - UnlockDoor

Test Case ID: DOORCONTROL-3

Profile C Requirement: Mandatory

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of door using UnlockDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with UnlockDoor operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes UnlockDoor request message to change the state of door.
2. Device responses with code HTTP 200 OK and UnlockDoorResponse message.

Test Result:

PASS -

- Client UnlockDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client UnlockDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<UnlockDoor>" tag after the "<Body>" tag AND
  - [S2] "<UnlockDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<UnlockDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_UnlockDoor

DOUBLE LOCK DOOR OPERATION

Test Label: Door Control - DoubleLockDoor

Test Case ID: DOORCONTROL-4

Profile C Requirement: Conditional

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of door using DoubleLockDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with DoubleLockDoor operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes DoubleLockDoor request message to change the state of door.
2. Device responses with code HTTP 200 OK and DoubleLockDoorResponse message.

Test Result:

PASS -

- Client DoubleLockDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client DoubleLockDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<DoubleLockDoor>" tag after the "<Body>" tag AND
  - [S2] "<DoubleLockDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<DoubleLockDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_DoubleLockDoor

BLOCK DOOR OPERATION

Test Label: Door Control - BlockDoor

Test Case ID: DOORCONTROL-5

Profile C Requirement: Conditional

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of door using BlockDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with BlockDoor operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes BlockDoor request message to change the state of door.

2. Device responses with code HTTP 200 OK and BlockDoorResponse message.

Test Result:

PASS -

- Client BlockDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client BlockDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<BlockDoor>" tag after the "<Body>" tag AND
  - [S2] "<BlockDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<BlockDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_BlockDoor

LOCK DOWN DOOR OPERATION

Test Label: Door Control - LockDownDoor

Test Case ID: DOORCONTROL-6

Profile C Requirement: Conditional

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of Door using LockDownDoor operation and then releasing this state using LockDownReleaseDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with LockDownDoor and LockDownReleaseDoor operations present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes LockDownDoor request message to change the state of door.
2. Device responses with code HTTP 200 OK and LockDownDoorResponse message.
3. Client invokes LockDownReleaseDoor request message to release the LockedDown state.
4. Device responses with code HTTP 200 OK and LockDownReleaseDoorResponse message.

Test Result:

PASS -

- Client LockDownDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client LockDownDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<LockDownDoor>" tag after the "<Body>" tag AND
  - [S2] "<LockDownDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<LockDownDoorResponse>" tag AND
- Client LockDownReleaseDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client LockDownReleaseDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S5] Client request contains "<LockDownReleaseDoor>" tag after the "<Body>" tag AND
  - [S6] "<LockDownReleaseDoor>" includes tag: "<Token>" with token value from LockDownDoor operation AND
  - [S7] Device response contains "HTTP/* 200 OK" AND
  - [S8] Device response contains "<LockDownReleaseDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_LockDownDoor

LOCK OPEN DOOR OPERATION

Test Label: Door Control - LockOpenDoor

Test Case ID: DOORCONTROL-7

Profile C Requirement: Conditional

Feature Under Test: Door Control

Test Purpose: To verify that Client is able to change the state of Door using LockOpenDoor operation and then releasing this state using LockOpenReleaseDoor operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with LockOpenDoor and LockOpenReleaseDoor operations present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes LockOpenDoor request message to change the state of door.
2. Device responses with code HTTP 200 OK and LockOpenDoorResponse message.
3. Client invokes LockOpenReleaseDoor request message to release the LockOpenDoor state.
4. Device responses with code HTTP 200 OK and LockOpenReleaseDoorResponse message.

Test Result:

PASS -

- Client LockOpenDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client LockOpenDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S1] Client request contains "<LockOpenDoor>" tag after the "<Body>" tag AND
  - [S2] "<LockOpenDoor>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<LockOpenDoorResponse>" tag. AND
- Client LockOpenReleaseDoor request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client LockOpenReleaseDoor request message has a proper hierarchy (refer to doorcontrol.wsdl) AND
  - [S5] Client request contains "<LockOpenReleaseDoor>" tag after the "<Body>" tag AND
  - [S6] "<LockOpenReleaseDoor>" includes tag: "<Token>" with token value from LockOpenDoor operation AND
  - [S7] Device response contains "HTTP/* 200 OK" AND
  - [S8] Device response contains "<LockOpenReleaseDoorResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: DoorControl_LockOpenDoor

Access Points Control Test Cases

Expected Scenarios Under Test:

1. Client invokes a specific Access Points Control commands in order to change the state of access point.
2. Client is considered as supporting Access Points Control if the following conditions are met:
   - Device returns a valid response to EnableAccessPoint request AND

  - Device returns a valid response to DisableAccessPoint request.

3. Client is considered as NOT supporting Access Points Control if ANY of the following is TRUE:
   - No valid Device response to EnableAccessPoint request OR
   - No valid Device response to DisableAccessPoint request.

DISABLE ENABLE ACCESS POINT OPERATION

Test Label: Access Points Control - DisableEnableAccessPoint

Test Case ID: ACCESSPOINTCONTROL-1

Profile C Requirement: Conditional

Feature Under Test: Access Points Control

Test Purpose: To verify that Client is able to disable Access Point using DisableAccessPoint operation and enable Access Point using EnableAccessPoint operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with DisableAccessPoint and EnableAccessPoint operations present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes DisableAccessPoint request message to disable Access Point.
2. Device responses with code HTTP 200 OK and DisableAccessPointResponse message.
3. Client invokes EnableAccessPoint request message to enable access point.
4. Device responses with code HTTP 200 OK and EnableAccessPointResponse message.

Test Result:

PASS -

- Client DisableAccessPoint request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client DisableAccessPoint request message has a proper hierarchy (refer to accesscontrol.wsdl) AND
  - [S1] Client request contains "<DisableAccessPoint>" tag after the "<Body>" tag AND
  - [S2] "<DisableAccessPoint>" includes tag: "<Token>" with non-empty string value of specific token AND
  - [S3] Device response contains "HTTP/* 200 OK" AND
  - [S4] Device response contains "<DisableAccessPointResponse>" tag AND
- Client EnableAccessPoint request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client EnableAccessPoint request message has a proper hierarchy (refer to accesscontrol.wsdl) AND
  - [S5] Client request contains "<EnableAccessPoint>" tag after the "<Body>" tag AND

- [S6] "<EnableAccessPoint>" includes tag: "<Token>" with token value from DisableAccessPoint operation AND
- [S7] Device response contains "HTTP/* 200 OK" AND
- [S8] Device response contains "<EnableAccessPointResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessPointsControl_DisableEnableAccessPoint

External Authorization Test Cases

Feature Level Requirement:

Validated Feature: ExternalAuthorization

Profile C Requirement: Conditional

Expected Scenarios Under Test:

1. Client subscribes to device messages using **CreatePullPointSubscription** operation.
2. Client receives authorization request from Device and makes a decision about granting access.
3. Client uses Pull Point event mechanism to retrieve notification events from Device.
4. Client receives notifications about access decisions related to External Authorization.
5. Client is considered as supporting External Authorization if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature AND
   - Client supports access_control_decisions feature AND
   - Client is able to receive authorization request from Device AND
   - Client is able to send authorization decision to Device using **ExternalAuthorization** operation.
6. Client is considered as NOT supporting External Authorization if ANY of the following is TRUE:
   - Client does not support EventHandling_Pullpoint feature OR
   - Client does not support access_control_decisions feature OR
   - Client unable to receive authorization request from Device OR
   - No Valid Device Response to **ExternalAuthorization** request.

RECEIVE AUTHORIZATION REQUEST

Test Label: External Authorization - Receive Authorization Request

Test Case ID: EXTERNALAUTHORIZATION-1

Profile C Normative Reference: Conditional

Feature Under Test: External Authorization

Test Purpose: To verify that Client is able to receive authorization request from Device using Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** and PullMessages operations present.
- The Network Trace Capture files contains at least one Conversation between Client and Device with **ExternalAuthorization** operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message without any filter or with appropriate filter.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.
3. Client invokes **PullMessages** command with Timeout and MessageLimit elements.
4. Device responses with code HTTP 200 OK and **PullMessagesResponse** message with corresponding event topic value.

Test Result:

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/Request/Credential** OR **tns1:AccessControl/Request/Anonymous** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/Request/Credential** OR **tns1:AccessControl/Request/Anonymous** OR **tns1:AccessControl/Request//.** OR **tns1:AccessControl//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND

- [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse** AND

- Client **PullMessages** request in Test Procedure fulfills the following requirements:
  - [S6] **soapenv:Body** element has child element **tev:PullMessages** AND
- Device response on the **PullMessages** request fulfills the following requirements:
  - [S7] It has HTTP 200 response code AND
  - [S8] **soapenv:Body** element has child element **tev:PullMessagesResponse** AND
  - [S9] A least one **wsnt:NotificationMessage/wsnt:Topic** element has value equal to EITHER **tns1:AccessControl/Request/Credential** OR **tns1:AccessControl/Request/Anonymous**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ExternalAuthorization_ReceiveAuthorizationRequest

SEND AUTHORIZATION DECISION

Test Label: External Authorization - Send Authorization Decision

Test Case ID: EXTERNALAUTHORIZATION-2

Profile C Normative Reference: Conditional

Feature Under Test: External Authorization

Test Purpose: To verify that Client is able to send Granted or Denied decision to Device.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with ExternalAuthorization operation present.

Test Procedure (expected to be reflected in network trace file):

1. Client sends ExternalAuthorization message to Device with Granted or Denied decision.
2. Device responses with code HTTP 200 OK and ExternalAuthorizationResponse message.

Test Result:

PASS -

- Client ExternalAuthorization request message is a well-formed SOAP request (refer to onvif.xsd) AND
- Client ExternalAuthorization request message has a proper hierarchy (refer to accesscontrol.wsdl) AND
  - [S1] Client request contains "<ExternalAuthorization>" tag after the "<Body>" tag AND
  - [S2] "<ExternalAuthorization>" includes tag: "<AccessPointToken>" with non-empty string value of specific token AND

- [S3] "<ExternalAuthorization>" includes tag: "<Decision>" AND
- [S4] "<Decision>" contains value EITHER ("Granted" OR "Denied") AND
- [S5] Device response contains "HTTP/* 200 OK" AND
- [S6] Device response contains "<ExternalAuthorizationResponse>" tag.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ExternalAuthorization_SendAuthorizationDecision

Access Control Decisions Test Cases

Feature Level Requirement:

Validated Feature: access_control_decisions

Profile C Requirement: Mandatory

Expected Scenarios Under Test:

1. Client subscribes to device messages using CreatePullPointSubscription operation to get Access Control Decisions notifications.
2. Client is considered as supporting Access Control Decisions if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature AND
   - Client supports SystemComponentInformation_AccessPointInfoList feature AND
   - Client is able to retrieve **tns1:AccessControl/AccessGranted/Credential** notifications AND
   - Client is able to retrieve **tns1:AccessControl/Denied/Credential** notifications AND
   - Client is able to retrieve **tns1:AccessControl/AccessGranted/Anonymous** notifications if Device supports AccessGrantedAnonymousEvent feature AND
   - Client is able to retrieve **tns1:AccessControl/Denied/Anonymous** notifications if Device supports AccessDeniedAnonymousEvent feature AND
   - Client is able to retrieve **tns1:AccessControl/Denied/CredentialNotFound/Card** notifications if Device supports AccessDeniedCredentialCredentialNotFoundCardEvent feature AND
   - Client is able to retrieve **tns1:AccessControl/AccessTaken/Credential** notifications if Device supports AccessTakenCredentialEvent feature AND
   - Client is able to retrieve **tns1:AccessControl/AccessTaken/Anonymous** notifications if Device supports AccessTakenAnonymousEvent feature AND
   - Client is able to retrieve **tns1:AccessControl/AccessNotTaken/Credential** notifications if Device supports AccessNotTakenCredentialEvent feature AND

- Client is able to retrieve **tns1:AccessControl/AccessNotTaken/Anonymous** notifications if Device supports AccessNotTakenAnonymousEvent feature.

3. Client is considered as NOT supporting Access Control Decisions if ANY of the following is TRUE:

- Client does not support EventHandling_Pullpoint feature OR
- Client does not support SystemComponentInformation_AccessPointInfoList feature OR
- Client unable to retrieve **tns1:AccessControl/AccessGranted/Credential** notifications OR
- Client unable to retrieve **tns1:AccessControl/Denied/Credential** notifications OR
- Client unable to retrieve **tns1:AccessControl/AccessGranted/Anonymous** notifications if Device supports AccessGrantedAnonymousEvent feature OR
- Client unable to retrieve **tns1:AccessControl/Denied/Anonymous** notifications if Device supports AccessDeniedAnonymousEvent feature OR
- Client unable to retrieve **tns1:AccessControl/Denied/CredentialNotFound/Card** notifications if Device supports AccessDeniedCredentialCredentialNotFoundCardEvent feature OR
- Client unable to retrieve **tns1:AccessControl/AccessTaken/Credential** notifications if Device supports AccessTakenCredentialEvent feature OR
- Client unable to retrieve **tns1:AccessControl/AccessTaken/Anonymous** notifications if Device supports AccessTakenAnonymousEvent feature OR
- Client unable to retrieve **tns1:AccessControl/AccessNotTaken/Credential** notifications if Device supports AccessNotTakenCredentialEvent feature OR
- Client unable to retrieve **tns1:AccessControl/AccessNotTaken/Anonymous** notifications if Device supports AccessNotTakenAnonymousEvent feature.

RETRIEVE ACCESS GRANTED WITH CREDENTIAL NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/AccessGranted/Credential event

Test Case ID: ACCESSCONTROLDECISIONS-1

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Granted with Credential notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/AccessGranted/Credential** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/AccessGranted/Credential** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/AccessGranted/Credential** OR **tns1:AccessControl/AccessGranted//.** OR **tns1:AccessControl//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessGrantedCredential

RETRIEVE ACCESS GRANTED TO ANONYMOUS NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/AccessGranted/Anonymous event

Test Case ID: ACCESSCONTROLDECISIONS-2

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Granted to Anonymous notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/AccessGranted/Anonymous** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessGrantedAnonymousEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND

- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):

    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/AccessGranted/Anonymous** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):

    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/AccessGranted/Anonymous** OR **tns1:AccessControl/AccessGranted//.** OR **tns1:AccessControl//.** in expression AND

- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:

  - [S4] It has HTTP 200 response code AND

  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

Validated Feature List: AccessControlDecisionRetrieval_AccessGrantedAnonymous

RETRIEVE ACCESS DENIED WITH CREDENTIAL NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/Denied/Credential event

Test Case ID: ACCESSCONTROLDECISIONS-3

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Denied with Credential notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/Denied/Credential** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND

- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):

    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/Denied/Credential** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):

    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/Denied/Credential** OR **tns1:AccessControl/Denied//.** OR **tns1:AccessControl//.** in expression AND

- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:

  - [S4] It has HTTP 200 response code AND

  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

Validated Feature List: AccessControlDecisionRetrieval_AccessDeniedCredential

RETRIEVE ACCESS DENIED TO ANONYMOUS NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/Denied/Anonymous event

Test Case ID: ACCESSCONTROLDECISIONS-4

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Denied to Anonymous notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/Denied/Anonymous** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

NOTE: In case when Device does not support **AccessDeniedAnonymousEvent** feature then Test shall be deemed as "PASSED" with this Device.

Test Result:

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/Denied/Anonymous** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/Denied/Anonymous** OR **tns1:AccessControl/Denied//.** OR **tns1:AccessControl//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessDeniedAnonymous

RETRIEVE ACCESS DENIED WITH CREDENTIAL (CREDENTIAL NOT FOUND – CARD) NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/Denied/CredentialNotFound/Card event

Test Case ID: ACCESSCONTROLDECISIONS-5

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Denied with Credential (Credential Not Found) notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/Denied/CredentialNotFound/Card** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessDeniedCredentialCredentialNotFoundCardEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND

- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):

    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/Denied/CredentialNotFound/Card** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):

- [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/Denied/CredentialNotFound/Card** OR **tns1:AccessControl/Denied/CredentialNotFound//.** OR **tns1:AccessControl/Denied//.** OR **tns1:AccessControl//.** in expression AND

- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessDeniedCredentialNotFoundCard

RETRIEVE ACCESS TAKEN WITH CREDENTIAL NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/AccessTaken/Credential event

Test Case ID: ACCESSCONTROLDECISIONS-6

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Taken with Credential notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/AccessTaken/Credential** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessTakenCredentialEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND

- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/AccessTaken/Credential** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/AccessTaken/Credential** OR **tns1:AccessControl/AccessTaken//.** OR **tns1:AccessControl//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessTakenCredential

RETRIEVE ACCESS TAKEN BY ANONYMOUS NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/AccessTaken/Anonymous event

Test Case ID: ACCESSCONTROLDECISIONS-7

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Taken by Anonymous notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/AccessTaken/Anonymous** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessTakenAnonymousEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/AccessTaken/Anonymous** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/AccessTaken/Anonymous** OR **tns1:AccessControl/AccessTaken//.** OR **tns1:AccessControl//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessTakenAnonymous

RETRIEVE ACCESS NOT TAKEN WITH CREDENTIAL NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/AccessNotTaken/Credential event

Test Case ID: ACCESSCONTROLDECISIONS-8

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Not Taken with Credential notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/AccessNotTaken/Credential** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessNotTakenCredentialEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/AccessNotTaken/Credential** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/AccessNotTaken/Credential** OR **tns1:AccessControl/AccessNotTaken//.** OR **tns1:AccessControl//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessNotTakenCredential

RETRIEVE ACCESS NOT TAKEN BY ANONYMOUS NOTIFICATIONS

Test Label: Retrieve Notifications about Access Control Decisions: tns1:AccessControl/AccessNotTaken/Anonymous event

Test Case ID: ACCESSCONTROLDECISIONS-9

Profile C Normative Reference: Mandatory

Feature Under Test: Access Control Decisions

Test Purpose: To verify that Client is able to retrieve Access Not Taken by Anonymous notifications from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/AccessNotTaken/Anonymous** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessNotTakenAnonymousEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND

- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):

    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/AccessNotTaken/Anonymous** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):

    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/AccessNotTaken/Anonymous** OR **tns1:AccessControl/AccessNotTaken//.** OR **tns1:AccessControl//.** in expression AND

- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:

  - [S4] It has HTTP 200 response code AND

  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: AccessControlDecisionRetrieval_AccessNotTakenAnonymous

Configuration Change Notifications Test Cases

Feature Level Requirement:

Validated Feature: configuration_change_notifications

Profile C Requirement: Mandatory

Expected Scenarios Under Test:

1. Client subscribes to device messages using **CreatePullPointSubscription** operation to get Configuration Change notifications.
2. Client uses Pull Point event mechanism to retrieve notification events from Device.
3. Client is considered as supporting Configuration change notification if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature AND
   - Client supports SystemComponentInformation_AccessPointInfoList feature AND
   - Client supports SystemComponentInformation_DoorInfoList feature AND
   - Client supports SystemComponentInformation_AreaInfoList feature AND
   - Client is able to retrieve **tns1:Configuration/AccessPoint/Changed** notifications if Device supports AccessPointChangedEvent feature AND
   - Client is able to retrieve **tns1:Configuration/AccessPoint/Removed** notifications if Device supports AccessPointRemovedEvent feature AND
   - Client is able to retrieve **tns1:Configuration/Door/Changed** notifications if Device supports DoorChangedEvent feature AND
   - Client is able to retrieve **tns1:Configuration/Door/Removed** notifications if Device supports DoorRemovedEvent feature AND
   - Client is able to retrieve **tns1:Configuration/Area/Changed** notifications if Device supports AreaChangedEvent feature AND
   - Client is able to retrieve **tns1:Configuration/Area/Removed** notifications if Device supports AreaRemovedEvent feature AND
4. Client is considered as NOT supporting Configuration change notification if ANY of the following is TRUE:
   - Client does not support EventHandling_Pullpoint feature OR
   - Client does not support SystemComponentInformation_AccessPointInfoList feature OR
   - Client does not support SystemComponentInformation_DoorInfoList feature OR
   - Client does not support SystemComponentInformation_AreaInfoList feature OR

- Client unable to retrieve **tns1:Configuration/AccessPoint/Changed** notifications if Device supports AccessPointChangedEvent feature OR
- Client unable to retrieve **tns1:Configuration/AccessPoint/Removed** notifications if Device supports AccessPointRemovedEvent feature OR
- Client unable to retrieve **tns1:Configuration/Door/Changed** notifications if Device supports DoorChangedEvent feature OR
- Client unable to retrieve **tns1:Configuration/Door/Removed** notifications if Device supports DoorRemovedEvent feature OR
- Client unable to retrieve **tns1:Configuration/Area/Changed** notifications if Device supports AreaChangedEvent feature OR
- Client unable to retrieve **tns1:Configuration/Area/Removed** notifications if Device supports AreaRemovedEvent feature.

RETRIEVE ACCESS POINTS CONFIGURATION CHANGED NOTIFICATIONS

Test Label: Retrieve Notifications about Acess Points Configuration Changed: tns1:Configuration/AccessPoint/Changed

Test Case ID: CONFIGURATIONCHANGENOTIFICATION-1

Profile C Normative Reference: Mandatory

Feature Under Test: Acess Points Configuration changed notification

Test Purpose: To verify that Client is able to retrieve notifications about configuration changes for access points or about added access point from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:Configuration/AccessPoint/Changed** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessPointChangedEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

- [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
- If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
  - [S2] **wsnt:TopicExpression** element is equal to **tns1:Configuration/AccessPoint/Changed** AND
- If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
  - [S3] **wsnt:TopicExpression** element contains **tns1:Configuration/AccessPoint/Changed** OR **tns1:Configuration/AccessPoint//.** OR **tns1:Configuration//.** in expression AND

- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ConfigurationMonitoring_AcessPointChanged

RETRIEVE ACCESS POINTS REMOVED NOTIFICATIONS

Test Label: Retrieve Notifications about Acess Points Removed: tns1:Configuration/AccessPoint/Removed

Test Case ID: CONFIGURATIONCHANGENOTIFICATION-2

Profile C Normative Reference: Mandatory

Feature Under Test: Acess Points Removed notification

Test Purpose: To verify that Client is able to retrieve notifications about remove of access points from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:Configuration/AccessPoint/Removed** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AccessPointRemovedEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:Configuration/AccessPoint/Removed** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:Configuration/AccessPoint/Removed** OR **tns1:Configuration/AccessPoint//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

Validated Feature List: ConfigurationMonitoring_AcessPointRemoved

RETRIEVE DOORS CONFIGURATION CHANGED NOTIFICATIONS

Test Label: Retrieve Notifications about Doors Configuration Changed: tns1:Configuration/Door/Changed

Test Case ID: CONFIGURATIONCHANGENOTIFICATION-3

Profile C Normative Reference: Mandatory

Feature Under Test: Doors Configuration changed notification

Test Purpose: To verify that Client is able to retrieve notifications about configuration changes for doors or about added doors from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:Configuration/Door/Changed** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.
2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **DoorChangedEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:Configuration/Door/Changed** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:Configuration/Door/Changed** OR **tns1:Configuration/Door//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ConfigurationMonitoring_DoorChanged

RETRIEVE DOORS REMOVED NOTIFICATIONS

Test Label: Retrieve Notifications about Doors Removed: tns1:Configuration/Door/Removed

Test Case ID: CONFIGURATIONCHANGENOTIFICATION-4

Profile C Normative Reference: Mandatory

Feature Under Test: Doors Removed notification

Test Purpose: To verify that Client is able to retrieve notifications about remove of doors from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:Configuration/Door/Removed** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **DoorRemovedEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:Configuration/Door/Removed** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:Configuration/Door/Removed** OR **tns1:Configuration/Door//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ConfigurationMonitoring_DoorRemoved

RETRIEVE AREAS CONFIGURATION CHANGED NOTIFICATIONS

Test Label: Retrieve Notifications about Areas Configuration Changed: tns1:Configuration/Area/Changed

Test Case ID: CONFIGURATIONCHANGENOTIFICATION-5

Profile C Normative Reference: Mandatory

Feature Under Test: Areas Configuration changed notification

Test Purpose: To verify that Client is able to retrieve notifications about configuration changes for areas or about added areas from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:Configuration/Area/Changed** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AreaChangedEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:Configuration/Area/Changed** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:Configuration/Area/Changed** OR **tns1:Configuration/Area//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ConfigurationMonitoring_AreaChanged

RETRIEVE AREAS REMOVED NOTIFICATIONS

Test Label: Retrieve Notifications about Areas Configuration Removed: tns1:Configuration/Area/Removed

Test Case ID: CONFIGURATIONCHANGENOTIFICATION-6

Profile C Normative Reference: Mandatory

Feature Under Test: Areas removed notification

Test Purpose: To verify that Client is able to retrieve notifications about remove of areas from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:Configuration/Area/Removed** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **AreaRemovedEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):
    - [S2] **wsnt:TopicExpression** element is equal to **tns1:Configuration/Area/Removed** AND
  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):
    - [S3] **wsnt:TopicExpression** element contains **tns1:Configuration/Area/Removed** OR **tns1:Configuration/Area//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: ConfigurationMonitoring_AreaRemoved

Duress Notifications Test Cases

Feature Level Requirement:

Validated Feature: configuration_change_notifications

Profile C Requirement: Mandatory

Expected Scenarios Under Test:

1. Client subscribes to device messages using **CreatePullPointSubscription** operation.
2. Client uses Pull Point event mechanism to retrieve notification events from Device.
3. Client is considered as supporting Duress notification if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature AND
   - Client supports SystemComponentInformation_AccessPointInfoList feature AND
   - Client is able to retrieve **tns1:AccessControl/Duress** notifications if Device supports DuressEvent feature.
4. Client is considered as NOT supporting Duress notification if ANY of the following is TRUE:
   - Client does not support EventHandling_Pullpoint feature OR
   - Client does not support SystemComponentInformation_AccessPointInfoList feature OR
   - Client unable to retrieve **tns1:AccessControl/Duress** notifications if Device supports DuressEvent feature.

RETRIEVE DURESS NOTIFICATIONS

Test Label: Retrieve Notifications About Duress: tns1:AccessControl/Duress

Test Case ID: DURESS-1

Profile C Normative Reference: Mandatory

Feature Under Test: Duress Situation Detected notification

Test Purpose: To verify that Client is able to retrieve notifications about duress situation detected at an access point from Device using the Pull Point event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreatePullPointSubscription** operations which do not filter out **tns1:AccessControl/Duress** event present.

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreatePullPointSubscription** message.

2. Device responses with code HTTP 200 OK and **CreatePullPointSubscriptionResponse** message.

Test Result:

NOTE: In case when Device does not support **DuressEvent** feature then Test shall be deemed as "PASSED" with this Device.

PASS -

- Client **CreatePullPointSubscription** request messages are valid according to XML Schemas listed in Namespaces AND

- Client **CreatePullPointSubscription** request in Test Procedure fulfills the following requirements:

  - [S1] **soapenv:Body** element has child element **tev:CreatePullPointSubscription** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete** then it fulfills the following requirements (else skip the check):

    - [S2] **wsnt:TopicExpression** element is equal to **tns1:AccessControl/Duress** AND

  - If it contains **tev:Filter/wsnt:TopicExpression** with **Dialect** attribute equal to **http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet** then it fulfills the following requirements (else skip the check):

    - [S3] **wsnt:TopicExpression** element contains **tns1:AccessControl/Duress** OR **tns1:AccessControl//.** in expression AND

- Device response on the **CreatePullPointSubscription** request fulfills the following requirements:

  - [S4] It has HTTP 200 response code AND

  - [S5] **soapenv:Body** element has child element **tev:CreatePullPointSubscriptionResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: Duress

A. Revision History

December 2, 2015 Version 16.01

- General item (Test Owerview) was added

- Minor updates in formatting, typos and terms according review result of other Client Test Specifications

- EXTERNALAUTHORIZATION-3 was removed. Related feature was chnaged in accordance.

- EXTERNALAUTHORIZATION-1 was updated to include new pre-requisite and new test style was upplied.

November 20, 2015 Version 16.01

- Change according to # 67:Expected Scenarios Under Test of Access Control Decisions, Configuration Change Notifications, Duress Notifications were updated: dependence on Device features were added. New Note was added into corresponding test cases.

September 28, 2015 Version 16.01

- Added Access Control Decisions Test Cases, Configuration Change Notifications, Duress Notifications Test Cases sections

June 10, 2015 Version 15.06

- No major changes were made, just minor formatting fixes.

May 20, 2015 Version 15.05

- No major changes were made, just minor grammatical corrections.

March 20, 2015 Version 15.03

- Added External Authorization Test Cases section.

February 19, 2015 Version 15.02

- Pass criteria in SYSTEMCOMPONENTSTATE-1 and 2 test cases have been updated (added additional criteria for checking <TopicExpression> tag value).

December 11, 2014 Version 14.12

- Fixed typos and inconsistencies.

November 21, 2014 Version 14.11

- Fixed typos and inconsistencies.
- Removed examples of expected Requests and Responses from all Test Cases.
- Removed unnecessary PASS criteria from all Test Cases.
- ACCESSPOINTCONTROL-1 and 2 test cases have been merged to the single ACCESSPOINTCONTROL-1 test case.
- DOORCONTROL-6 and 7 test cases have been merged to the single DOORCONTROL-6 test case.
- DOORCONTROL-8 and 9 test cases have been merged to the single DOORCONTROL-7 test case.
- SYSTEMCOMPONENTINFORMATION-1, 2 and 3 test cases have been updated.
- "7.1. Expected Scenarios Under Test" section has been updated.
- "3. Terms and Definitions" section has been updated.
- Introduced YY.MM method of version numbering

October 16, 2014 Version 1.0

- Initial version