ONVIF Profile A 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 [http://www.onvif.org/Documents/Specifications.aspx]).

This particular document defines test cases required for testing Profile A features of a Client application e.g. Get Credentials Capabilities, Get Credentials List, Get Credentials Details, Configure Credentials, Credential Configuration and State Notifications, Get Schedules List, Schedule Configuration Notifications, Get Access Profiles, Access Profile Configuration Notifications. It also describes the test framework, test setup, prerequisites, test policies needed for the execution of the described test cases.

Scope

This ONVIF Profile A Client Test Specification defines and regulates the conformance testing procedure for the ONVIF conformant Clients in the scope of Profile A 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 A features according to ONVIF Profile Specifications.

The principal intended purposes are:

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

Get Credential Capabilities

Get Credential Capabilities section specifies Client ability to request lcapabilities of Credential Service from Device.

Get Credentials List

Get Credentials List section specifies Client ability to request lists of Credentials from Device.

Get Credentials Details

Get Credentials Details section specifies Client ability to request detailed information about Credentials.

Configure Credentials

Configure Credentials section specifies Client ability configure Credentials on Device.

Credential Configuration and State Notifications

Credential Configuration and State Notifications section specifies Client ability to receive from Device configuration and state notifications for Credentials.

Get Schedules List

Get Schedules List section specifies Client ability to request lists of Schedules from Device.

Schedule Configuration Notifications

Schedule Configuration Notifications section specifies Client ability to receive from Device configuration notifications for Schedules.

Get Access Profiles List

Get Access Profiles List section specifies Client ability to request lists of Access Profiles from Device.

Access Profile Configuration Notifications

Access Profile Configuration Notifications section specifies Client ability to receive from Device configuration notifications for Access Profiles.

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

WS-BaseNotification:

http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.pdf

W3C SOAP 1.2, Part 1, Messaging Framework:

http://www.w3.org/TR/soap12-part1/

W3C XML Schema Part 1: Structures Second Edition:

http://www.w3.org/TR/xmlschema-1/

W3C XML Schema Part 2: Datatypes Second Edition:

"http://www.w3.org/TR/xmlschema-2/ [http://www.w3.org/TR/xmlschema-2/]

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 A The Profile A 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.
Access Policy	An association of an access point and a schedule. An access policy defines when an access point can be accessed using an access profile which contains this access policy.
Access Profile	A collection of access policies, used to define role based access.
Access Point	A logical composition of a physical door and ID point(s) controlling access in one direction.
Credential	A physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system.
Validity Period	From a certain point in time, to a later point in time.
Schedule	A set of time periods, for example: working hours (weekdays from 08:00 AM to 06:00 PM). It may also include one or more special days schedule.
ID Point	A device that converts reader signals to protocols recognized by an authorization engine. It can be card reader, REX, biometric reader etc.

Anti-Passback	Operating mode which requires user validation when leaving a security controlled area in order to be able to re-enter and vice versa.
Anti-Passback Violation State	A signal stating if the anti-passback rules have been violated for a credential.
Credential Format	The credential data can be formatted in many different ways. ONVIF supports the BACnet format types in [ISO 16484-5:2014-09 Annex P].
Credential Holder	Associates a credential with a user. Typically it holds a reference to a credential and a reference to a user.
Credential Identifier	Card number, unique card information, PIN, fingerprint, or other biometric information, etc., that can be validated in an access point.
Credential Number	A sequence of bytes uniquely identifying a credential at an access point.
Credential State	The credential state indicates if a credential is enabled or disabled. The state also indicates if anti-passback has been violated or not. The state may also contain a reason why the credential was disabled.
Duress	Forcing a person to provide access to a secure area against that person's wishes.
Format Type	See Credential Format.
iCalendar	An industry standard format for exchanging scheduling and activity-recording information electronically.
Special Days	A set of dates that require the regular Schedule to be overridden, e.g. holidays, half-days or working Sundays.
Special Days Schedule	A schedule that defines time periods for a Special Day List.
Time Period	A time period has a start time and an end time, e.g. 8 AM to 6 PM.
vEvent	A component in iCalendar, specifying the properties of an event.
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.
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
tds	http://www.onvif.org/ver10/device/wsdl	The namespace for the WSDL device service
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
tas	http://www.onvif.org/ver10/advancedsecurity/wsdl	The namespace for the WSDL advanced security service
tar	http://www.onvif.org/ver10/accessrules/wsdl	The namespace for the WSDL access rules service
tcr	http://www.onvif.org/ver10/credential/wsdl	The namespace for the WSDL credential service
tsc	http://www.onvif.org/ver10/schedule/wsdl	The namespace for the WSDL schedule service
wsnt	http://docs.oasis-open.org/wsn/b-2	Schema namespace of the [WS-BaseNotification] specification.

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 compliant to PACS Profile A can provide configurations of access rules, credentials and schedules. The 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 Normative Reference
- Expected Scenarios Under Test
- List of Test Cases

Feature Level Normative Reference

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

If Feature Level Normative Reference 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 Normative Reference 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 - Normative Reference 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 A, 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.

Get Credential Capabilities Test Cases

Feature Level Normative Reference:

Validated Feature: get_credential_capabilities

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client connects to Device to retrieve a credential service capabilities.
2. Client is considered as supporting Get Credential Capabilities if the following conditions are met:
   - Client is able to retrieve a credential service capabilities using **GetServiceCapabilities** operation (Credential Service) OR supports get_services_capabilities.get_services feature.
3. Client is considered as NOT supporting Get Credential Capabilities if ANY of the following is TRUE:
   - No valid response **GetServiceCapabilities** request (Credential Service) AND get_credential_capabilities.get_services feature is not supported by Client.

GET SERVICE CAPABILITIES

Test Label: Get Credential Capabilities - Get Service Capabilities

Test Case ID: GETCREDENTIALCAPABILITIES-1

Profile A Normative Reference: Optional

Feature Under Test: Get Services

Test Purpose: To verify that credential service capabilities provided by Device is received by Client using the **GetServiceCapabilities** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetServiceCapabilities** operation for Credential Service present.
- Device supports Credential Service.

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

1. Client invokes **GetServiceCapabilities** request message to retrieve credential service capabilities from the Device.
2. Device responses with code HTTP 200 OK and **GetServiceCapabilitiesResponse** message.

Test Result:

PASS -

- Client **GetServiceCapabilities** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **GetServiceCapabilities** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tcr:GetServiceCapabilities** AND
- Device response on the **GetServiceCapabilities** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND
  - [S3] **soapenv:Body** element has child element **tcr:GetServiceCapabilitiesResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_credential_capabilities.get_service_capabilities

Get Credentials List Test Cases

Feature Level Normative Reference:

Validated Feature: get_credential_list

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client connects to Device to retrieve a complete list of Credentials.
2. Client is considered as supporting Get Credentials List if the following conditions are met:
   - Client is able to list available Credentials using **GetCredentialInfoList** operation OR **GetCredentialList** operation.
3. Client is considered as NOT supporting Get Credentials List if ANY of the following is TRUE:

- No valid responses for **GetCredentialInfoList** request OR **GetCredentialList** request OR
- **GetCredentialInfoList** request contains **tcr:StartReference** element value that was not recieved in **GetCredentialInfoList** response in **tcr:NextStartReference** element OR
- **GetCredentialList** request contains **tcr:StartReference** element value that was not recieved in **GetCredentialList** response in **tcr:NextStartReference** element OR
- Complete Credentials list was not received.

LISTING OF CREDENTIALS

Test Label: Get Credentials List - Listing of Credentials

Test Case ID: GETCREDENTIALLIST-1

Profile A Normative Reference: Optional

Feature Under Test: Get Credentials List

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

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetCredentialList** operation present.
- Device supports Credential Service.

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

1. Client invokes **GetCredentialList** request message with skipped **tcr:StartReference** element to retrieve first part of the list of all credentials configured on the Device.
2. Device responses with code HTTP 200 OK and **GetCredentialListResponse** message.
3. If **GetCredentialListResponse** message contains **tcr:NextStartReference** element Client invokes **GetCredentialList** request message with **tcr:StartReference** element equal to value of **tcr:NextStartReference** element to retrieve next part of the list of all credentials configured on the Device.
4. Client repeats the previous step while **GetCredentialListResponse** message contains **tcr:NextStartReference** element.

Test Result:

PASS -

- Client **GetCredentialList** request messages are valid according to XML Schemas listed in Namespaces AND
- First Client **GetCredentialList** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tcr:GetCredentialList** AND

- [S2] It does not contain **tcr:StartReference** element AND

- If response on previous **GetCredentialList** request contains **tcr:NextStartReference** element each next Client **GetCredentialList** requests in Test Procedure fulfills the following requirements (else skip the checks):

  - [S3] **soapenv:Body** element has child element **tcr:GetCredentialList** AND

  - [S4] It contains **tcr:StartReference** element equal to **tcr:NextStartReference** element from response on previous **GetCredentialList** request AND

- Device responses on the each **GetCredentialList** request in Test Procedure fulfills the following requirements:

  - [S5] It has HTTP 200 response code AND

  - [S6] **soapenv:Body** element has child element **tcr:GetCredentialListResponse** AND

- The last in Test Procedure Device response on **GetCredentialList** request fulfills the following requirements:

  - [S7] It does not contain **tcr:NextStartReference** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_credential_list.get_credential_list

LISTING OF CREDENTIAL INFO

Test Label: Get Credentials List - Listing of Credential Info

Test Case ID: GETCREDENTIALLIST-2

Profile A Normative Reference: Mandatory

Feature Under Test: Get Credential Info List

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

Pre-Requisite:

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

- Device supports Credential Service.

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

1. Client invokes **GetCredentialInfoList** request message with skipped **tcr:StartReference** element to retrieve first part of the list of all credentials configured on the Device.

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

3. If **GetCredentialInfoListResponse** message contains **tcr:NextStartReference** element Client invokes **GetCredentialInfoList** request message with **tcr:StartReference** element equal to value of **tcr:NextStartReference** element to retrieve next part of the list of all credentials configured on the Device.

4. Client repeats the previous step while **GetCredentialInfoListResponse** message contains **tcr:NextStartReference** element.

Test Result:

PASS -

- Client **GetCredentialInfoList** request messages are valid according to XML Schemas listed in Namespaces AND
- First Client **GetCredentialInfoList** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tcr:GetCredentialInfoList** AND
  - [S2] It does not contain **tcr:StartReference** element AND
- If response on previous **GetCredentialInfoList** request contains **tcr:NextStartReference** element each next Client **GetCredentialInfoList** requests in Test Procedure fulfills the following requirements (else skip the checks):
  - [S3] **soapenv:Body** element has child element **tcr:GetCredentialInfoList** AND
  - [S4] It contains **tcr:StartReference** element equal to **tcr:NextStartReference** AND element from response on previous **GetCredentialInfoList** request AND
- Device responses on the each **GetCredentialInfoList** request in Test Procedure fulfills the following requirements:
  - [S5] It has HTTP 200 response code AND
  - [S6] **soapenv:Body** element has child element **tcr:GetCredentialInfoListResponse** AND
- The last in Test Procedure Device response on **GetCredentialInfoList** request fulfills the following requirements:
  - [S7] It does not contain **tcr:NextStartReference** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_credential_list.get_credential_info_list

Get Credentials Details Test Cases

Feature Level Normative Reference:

Validated Feature: get_credential_details

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client connects to Device to retrieve a Credentials details.
2. Client is considered as supporting Get Credentials Details if the following conditions are met:
   - Client is able to get Credentials details using **GetCredentials** operation OR Client supports get_credential_list.get_credential_list feature.
3. Client is considered as NOT supporting Get Credentials Details if ANY of the following is TRUE:
   - No valid responses for **GetCredentials** request with at least one Credential listed in it.

GET CREDENTIALS

Test Label: Get Credentials Details - Get Credentials

Test Case ID: GETCREDENTIALDETAILS-1

Profile A Normative Reference: Mandatory

Feature Under Test: Get Credentials

Test Purpose: To verify that credential details provided by Device is received by Client using the **GetCredentials** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetCredentials** operation present.
- Device supports Credential Service.

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

1. Client invokes **GetCredentials** request message to retrieve credential details for specified credentials from the Device.
2. Device responses with code HTTP 200 OK and **GetCredentialsResponse** message which contains at least one **tcr:Credential** element.

Test Result:

PASS -

- Client **GetCredentials** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **GetCredentials** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tcr:GetCredentials** AND
- Device response on the **GetCredentials** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND

- [S3] **soapenv:Body** element has child element **tcr:GetCredentialsResponse** AND
- [S4] It contains at least one **tcr:Credential** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_credential_details.get_credentials

Configure Credentials Test Cases

Feature Level Normative Reference:

Validated Feature: configure_credentials

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client supports get_credential_capabilities feature.
2. Client get supported format types of a specified identifier type using **GetSupportedFormatTypes** operation to use it for **CreateCredential** operation and **ModifyCredential** operation.
3. Client creates credentials on a Device using **CreateCredential** operation.
4. Client modifys credentials on a Device using **ModifyCredential** operation.
5. Client deletes credentials from a Device using **DeleteCredential** operation.
6. Client is considered as supporting Configure Credentials if the following conditions are met:
   - Client is able to get supported idetifier types using **GetServiceCapabilities** operation or **GetServices** operation AND
   - Client is able to get supported format types of a specified identifier type using **GetSupportedFormatTypes** operation AND
   - Client is able to create credential using **CreateCredential** operation AND
   - Client is able to modify credential using **ModifyCredential** operation AND
   - Client is able to delete credential using **DeleteCredential** operation.
7. Client is considered as NOT supporting Configure Credentials if ANY of the following is TRUE:
   - No valid responses for **GetSupportedFormatTypes** request OR
   - No valid responses for **CreateCredential** request OR
   - No valid responses for **ModifyCredential** request OR
   - No valid responses for **DeleteCredential** request.

GET SUPPORTED FORMAT TYPES

Test Label: Configure Credentials - Get Supported Format Types

Test Case ID: CONFIGURECREDENTIALS-1

Profile A Normative Reference: Mandatory

Feature Under Test: Get Supported Format Types

Test Purpose: To verify that Client is able to get supported format types from Device for specified identifier type using the **GetSupportedFormatTypes** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetSupportedFormatTypes** operation present.
- Device supports Credential Service.

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

1. Client invokes **GetSupportedFormatTypes** request message to get supported format types from Device for specified identifier type.
2. Device responses with code HTTP 200 OK and **GetSupportedFormatTypesResponse** message.

Test Result:

PASS -

- Client **GetSupportedFormatTypes** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **GetSupportedFormatTypes** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tcr:GetSupportedFormatTypes** AND
- Device response on the **GetSupportedFormatTypes** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND
  - [S3] **soapenv:Body** element has child element **tcr:GetSupportedFormatTypesResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: configure_credentials.get_supported_format_types

CREATE CREDENTIAL

Test Label: Configure Credentials - Create Credential

Test Case ID: CONFIGURECREDENTIALS-2

Profile A Normative Reference: Mandatory

Feature Under Test: Create Credential

Test Purpose: To verify that Client is able to create credential on Device using the **CreateCredential** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **CreateCredential** operation present.
- Device supports Credential Service.

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

1. Client invokes **GetSupportedFormatTypes** request message to get supported format types from Device for specified identifier type.
2. Device responses with code HTTP 200 OK and **GetSupportedFormatTypesResponse** message.
3. Client invokes **CreateCredential** request message to create credential on Device with identifier type from **GetSupportedFormatTypes** request message and format type from **GetSupportedFormatTypes** response message.
4. Device responses with code HTTP 200 OK and **CreateCredentialResponse** message.

Test Result:

PASS -

- Client **CreateCredential** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreateCredential** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child **tcr:CreateCredential** element AND
  - [S2] **tcr:Credential/@token** attribute is empty (has empty string value) AND
  - [S3] IF it contains **tcr:Credential/tcr:ValidFrom** element AND **tcr:Credential/tcr:ValidTo** element THEN **tcr:ValidFrom** element value is less or equal to **tcr:ValidTo** element value AND
  - [S4] IF there is at least one **tcr:Credential/tcr:CredentialAccessProfile** element with child elements **tcr:ValidFrom** AND **tcr:ValidTo** THEN for all such **tcr:Credential/tcr:CredentialAccessProfile** elements **tcr:ValidFrom** element value is less or equal to **tcr:ValidTo** element value AND
- Device response on the **CreateCredential** request fulfills the following requirements:
  - [S5] It has HTTP 200 response code AND
  - [S6] **soapenv:Body** element has child element **tcr:CreateCredentialResponse** AND
- For each **tcr:Credential/tcr:CredentialIdentifier** from the **CreateCredential** request in Test Procedure fulfills the following requirements:
  - There is a Client **GetSupportedFormatTypes** request in Test Procedure fulfills the following requirements:
    - [S7] It invoked for the same Device as for the Client **CreateCredential** request AND

- [S8] It invoked before the Client **CreateCredential** request AND
- [S9] **tcr:CredentialIdentifierTypeName** element value is equal to **tcr:Credential/ tcr:CredentialIdentifier/tcr:Type/tcr:Name** element from the **CreateCredential** request AND

- Device response on the **GetSupportedFormatTypes** request fulfills the following requirements:
  - [S10] It has HTTP 200 response code AND
  - [S11] There is **tcr:FormatTypeInfo/tcr:FormatType** element which value is equal to **tcr:Credential/tcr:CredentialIdentifier/tcr:Type/tcr:FormatType** element value for the corresponding **tcr:Credential/tcr:CredentialIdentifier** element from the **CreateCredential** request with **tcr:Credential/tcr:CredentialIdentifier/tcr:Type/tcr:Name** element value equal to **tcr:CredentialIdentifierTypeName** element value from the **GetSupportedFormatTypes** request.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: configure_credentials.create_credential

MODIFY CREDENTIAL

Test Label: Configure Credentials - Modify Credential

Test Case ID: CONFIGURECREDENTIALS-3

Profile A Normative Reference: Mandatory

Feature Under Test: Modify Credential

Test Purpose: To verify that Client is able to modify credential on Device using the **ModifyCredential** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **ModifyCredential** operation present.
- Device supports Credential Service.

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

1. Client invokes **ModifyCredential** request message to create credential on Device.
2. Device responses with code HTTP 200 OK and **ModifyCredentialResponse** message.

Test Result:

PASS -

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

- [S1] **soapenv:Body** element has child **tcr:ModifyCredential** element AND
- If it contains **tcr:Credential/tcr:ValidFrom** element AND **tcr:Credential/tcr:ValidTo** element then it fulfills the following requirements (else skip the checks):
  - [S2] **tcr:Credential/tcr:ValidFrom** element value is less or equal to **tcr:Credential/tcr:ValidTo** element value AND
- If it contains at least one **tcr:Credential/tcr:CredentialAccessProfile** with child elements **tcr:ValidFrom** AND **tcr:ValidTo** then it fulfills the following requirements (else skip the checks):
  - [S3] For all **tcr:Credential/tcr:CredentialAccessProfile** elements with child elements **tcr:ValidFrom** AND **tcr:ValidTo tcr:ValidFrom** element value is less or equal to **tcr:ValidTo** element value AND

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

FAIL -

- The Client failed PASS criteria.

Validated Feature List: configure_credentials.modify_credential

DELETE CREDENTIAL

Test Label: Configure Credentials - Delete Credential

Test Case ID: CONFIGURECREDENTIALS-4

Profile A Normative Reference: Mandatory

Feature Under Test: Delete Credential

Test Purpose: To verify that Client is able to delete credential from Device using the **DeleteCredential** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **DeleteCredential** operation present.
- Device supports Credential Service.

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

1. Client invokes **DeleteCredential** request message to delete credential from the Device for specified credential.
2. Device responses with code HTTP 200 OK and **DeleteCredentialResponse** message.

Test Result:

PASS -

- Client **DeleteCredential** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **DeleteCredential** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tcr:DeleteCredential** AND
- Device response on the **DeleteCredential** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND
  - [S3] **soapenv:Body** element has child element **tcr:DeleteCredentialResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: configure_credentials.delete_credential

Credential Configuration and State Notifications Test Cases

Feature Level Normative Reference:

Validated Feature: credentials_notifications

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client subscribes to device messages using **CreatePullPointSubscription** operation OR **Subscribe** operation to get credentials configuration notifications.
2. Client subscribes to device messages using **CreatePullPointSubscription** operation OR **Subscribe** operation to get credentials state notifications.
3. Client uses Pull Point event mechanism OR Basic Notification event mechanism (if Device supports Basic Notification event mechanism) to retrieve notification events from Device.
4. Client is considered as supporting Credential Configuration and State Notifications if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature OR EventHandling_WS-BaseNotification feature AND
   - Client supports get_credential_list feature AND
   - Client is able to retrieve notifications about credential configuration change AND
   - Client is able to retrieve notifications about credential removing AND
   - Client is able to retrieve notifications about credential enable state change.
5. Client is considered as NOT supporting Credential Configuration and State Notifications if ANY of the following is TRUE:

- Client does not support EventHandling_Pullpoint feature AND EventHandling_WS-BaseNotification feature OR
- Client does not support get_credential_list feature OR
- Client is not able to retrieve notifications about credential configuration change OR
- Client is not able to retrieve notifications about credential removing OR
- Client is not able to retrieve notifications about credential enable state change.

RETRIEVE CREDENTIAL CONFIGURATION CHANGED NOTIFICATIONS - PULL POINT

Test Label: Retrieve Credential Configuration Changed Notifications - Pull Point

Test Case ID: CREDENTIALNOTIFICATIONS-1

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Configuration/Credential/Changed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about credential configuration changes 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 present wich is not filter out notification with topic **tns1:Configuration/Credential/Changed**.
- Device supports Credential Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Configuration/Credential/Changed** notifications from the Device.
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:Configuration/Credential/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/Credential/Changed** OR **tns1:Configuration/Credential//.** 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: credentials_notifications.configuration_credential_changed

RETRIEVE CREDENTIAL CONFIGURATION REMOVED NOTIFICATIONS - PULL POINT

Test Label: Retrieve Credential Configuration Removed Notifications - Pull Point

Test Case ID: CREDENTIALNOTIFICATIONS-2

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Configuration/Credential/Removed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about credential configuration removing 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 present wich is not filter out notification with topic **tns1:Configuration/Credential/Removed**.
- Device supports Credential Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Configuration/Credential/Removed** notifications from the Device.
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:Configuration/Credential/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/Credential/Removed** OR **tns1:Configuration/Credential//.** 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: credentials_notifications.configuration_credential_removed

RETRIEVE CREDENTIAL ENABLE STATE NOTIFICATIONS - PULL POINT

Test Label: Retrieve Credential Enable State Notifications - Pull Point

Test Case ID: CREDENTIALNOTIFICATIONS-3

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Credential/State/Enabled** Notification

Test Purpose: To verify that Client is able to retrieve notifications about credential enable state 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 present wich is not filter out notification with topic **tns1:Credential/State/Enabled**.
- Device supports Credential Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Credential/State/Enabled** notifications from the Device.
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:Credential/State/Enabled** 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:Credential/State/Enabled** OR **tns1:Credential/State//.** OR **tns1:Credential//.** 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: credentials_notifications.credential_state_enabled

RETRIEVE CREDENTIAL CONFIGURATION CHANGED NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Credential Configuration Changed Notifications - Basic Notification

Test Case ID: CREDENTIALNOTIFICATIONS-4

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Configuration/Credential/Changed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about credential configuration changes from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic **tns1:Configuration/Credential/Changed**.
- Device supports Credential Service.

- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Configuration/Credential/Changed** notifications from the Device.

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

Test Result:

PASS -

- Client **Subscribe** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **Subscribe** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **wsnt:Subscribe** AND
  - If it contains **wsnt: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/Credential/Changed** AND
  - If it contains **wsnt: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/Credential/Changed** OR **tns1:Configuration/Credential//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **Subscribe** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **wsnt:SubscribeResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: credentials_notifications.configuration_credential_changed_bn

RETRIEVE CREDENTIAL CONFIGURATION REMOVED NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Credential Configuration Removed Notifications - Basic Notification

Test Case ID: CREDENTIALNOTIFICATIONS-5

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Configuration/Credential/Removed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about credential configuration removing from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic **tns1:Configuration/Credential/Removed**.
- Device supports Credential Service.
- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Configuration/Credential/Removed** notifications from the Device.
2. Device responses with code HTTP 200 OK and **SubscribeResponse** message.

Test Result:

PASS -

- Client **Subscribe** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **Subscribe** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **wsnt:Subscribe** AND
  - If it contains **wsnt: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/Credential/Removed** AND
  - If it contains **wsnt: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/Credential/Removed** OR **tns1:Configuration/Credential//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **Subscribe** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **wsnt:SubscribeResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: credentials_notifications.configuration_credential_removed_bn

RETRIEVE CREDENTIAL ENABLE STATE NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Credential Enable State Notifications - Basic Notification

Test Case ID: CREDENTIALNOTIFICATIONS-6

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Credential/State/Enabled** Notification

Test Purpose: To verify that Client is able to retrieve notifications about credential enable state from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic tns1:Credential/State/Enabled.
- Device supports Credential Service.
- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Credential/State/Enabled** notifications from the Device.
2. Device responses with code HTTP 200 OK and **SubscribeResponse** message.

Test Result:

PASS -

- Client **Subscribe** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **Subscribe** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **wsnt:Subscribe** AND
  - If it contains **wsnt: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:Credential/State/Enabled** AND
  - If it contains **wsnt: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:Credential/State/Enabled** OR **tns1:Credential/State//.** OR **tns1:Credential//.** in expression AND
- Device response on the **Subscribe** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **wsnt:SubscribeResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: credentials_notifications.credential_state_enabled_bn

Get Schedules List Test Cases

Feature Level Normative Reference:

Validated Feature: get_schedule_list

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client connects to Device to retrieve a complete list of Schedules.
2. Client is considered as supporting Get Schedules List if the following conditions are met:
   - Client is able to list available Schedules using **GetScheduleInfoList** operation OR **GetScheduleList** operation.
3. Client is considered as NOT supporting Get Schedules List if ANY of the following is TRUE:
   - No valid responses for **GetScheduleInfoList** request OR **GetScheduleList** request OR
   - **GetScheduleInfoList** request contains **tsc:StartReference** element value that was not recieved in **GetScheduleInfoList** response in **tsc:NextStartReference** element OR
   - **GetScheduleList** request contains **tsc:StartReference** element value that was not recieved in **GetScheduleList** response in **tsc:NextStartReference** element OR
   - Complete Schedules list was not received.

LISTING OF SCHEDULES

Test Label: Get Schedules List - Listing of Schedules

Test Case ID: GETSCHEDULELIST-1

Profile A Normative Reference: Optional

Feature Under Test: Get Schedules List

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

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetScheduleList** operation present.
- Device supports Schedule Service.

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

1. Client invokes **GetScheduleList** request message with skipped **tsc:StartReference** element to retrieve first part of the list of all schedules configured on the Device.

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

3. If **GetScheduleListResponse** message contains **tsc:NextStartReference** element Client invokes **GetScheduleList** request message with **tsc:StartReference** element equal to value of **tsc:NextStartReference** element to retrieve next part of the list of all schedules configured on the Device.

4. Client repeats the previous step while **GetScheduleListResponse** message contains **tsc:NextStartReference** element.

Test Result:

PASS -

- Client **GetScheduleList** request messages are valid according to XML Schemas listed in Namespaces AND
- First Client **GetScheduleList** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tsc:GetScheduleList** AND
  - [S2] It does not contain **tsc:StartReference** element AND
- If response on previous **GetScheduleList** request contains **tcr:NextStartReference** element each next Client **GetScheduleList** requests in Test Procedure fulfills the following requirements (else skip the checks):
  - [S3] **soapenv:Body** element has child element **tsc:GetScheduleList** AND
  - [S4] It contains **tsc:StartReference** element equal to **tsc:NextStartReference** element from response on previous **GetScheduleList** request AND
- Device responses on the each **GetScheduleList** request in Test Procedure fulfills the following requirements:
  - [S5] It has HTTP 200 response code AND
  - [S6] **soapenv:Body** element has child element **tsc:GetScheduleListResponse** AND
- The last in Test Procedure Device response on **GetScheduleList** request fulfills the following requirements:
  - [S7] It does not contain **tcr:NextStartReference** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_schedule_list.get_schedule_list

LISTING OF SCHEDULE INFO

Test Label: Get Schedules List - Listing of Schedule Info

Test Case ID: GETSCHEDULELIST-2

Profile A Normative Reference: Mandatory

Feature Under Test: Get Schedule Info List

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

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetScheduleInfoList** operation present.
- Device supports Schedule Service.

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

1. Client invokes **GetScheduleInfoList** request message with skipped **tsc:StartReference** element to retrieve first part of the list of all schedules configured on the Device.
2. Device responses with code HTTP 200 OK and **GetScheduleInfoListResponse** message.
3. If **GetScheduleInfoListResponse** message contains **tsc:NextStartReference** element Client invokes **GetScheduleInfoList** request message with **tsc:StartReference** element equal to value of **tsc:NextStartReference** element to retrieve next part of the list of all schedules configured on the Device.
4. Client repeats the previous step while **GetScheduleInfoListResponse** message contains **tsc:NextStartReference** element.

Test Result:

PASS -

- Client **GetScheduleInfoList** request messages are valid according to XML Schemas listed in Namespaces AND
- First Client **GetScheduleInfoList** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tsc:GetScheduleInfoList** AND
  - [S2] It does not contain **tsc:StartReference** element AND
- If response on previous **GetScheduleInfoList** request contains **tcr:NextStartReference** element each next Client **GetScheduleInfoList** requests in Test Procedure fulfills the following requirements (else skip the checks):
  - [S3] **soapenv:Body** element has child element **tsc:GetScheduleInfoList** AND
  - [S4] It contains **tsc:StartReference** element equal to **tsc:NextStartReference** element from response on previous **GetScheduleInfoList** request AND
- Device responses on the each **GetScheduleInfoList** request in Test Procedure fulfills the following requirements:
  - [S5] It has HTTP 200 response code AND
  - [S6] **soapenv:Body** element has child element **tsc:GetScheduleInfoListResponse** AND
- The last in Test Procedure Device response on **GetScheduleInfoList** request fulfills the following requirements:

- [S7] It does not contain **tcr:NextStartReference** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_schedule_list.get_schedule_info_list

Schedule Configuration Notifications Test Cases

Feature Level Normative Reference:

Validated Feature: schedules_notifications

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client subscribes to device messages using **CreatePullPointSubscription** operation OR **Subscribe** operation to get schedules configuration notifications.
2. Client uses Pull Point event mechanism OR Basic Notification event mechanism (if Device supports Basic Notification event mechanism) to retrieve notification events from Device.
3. Client is considered as supporting Schedule Configuration if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature OR EventHandling_WS-BaseNotification feature AND
   - Client supports get_schedule_list feature AND
   - Client is able to retrieve notifications about schedule configuration change AND
   - Client is able to retrieve notifications about schedule removing AND
4. Client is considered as NOT supporting Schedule Configuration and State Notifications if ANY of the following is TRUE:
   - Client does not support EventHandling_Pullpoint feature AND EventHandling_WS-BaseNotification feature OR
   - Client does not support get_schedule_list feature OR
   - Client is not able to retrieve notifications about schedule configuration change OR
   - Client is not able to retrieve notifications about schedule removing.

RETRIEVE SCHEDULE CONFIGURATION CHANGED NOTIFICATIONS - PULL POINT

Test Label: Retrieve Schedule Configuration Changed Notifications - Pull Point

Test Case ID: SCHEDULENOTIFICATIONS-1

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Configuration/Schedule/Changed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about schedule configuration changes 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 present wich is not filter out notification with topic **tns1:Configuration/Schedule/Changed**.
- Device supports Schedule Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Configuration/Schedule/Changed** notifications from the Device.
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:Configuration/Schedule/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/Schedule/Changed** OR **tns1:Configuration/Schedule//.** 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: schedules_notifications.configuration_schedule_changed

RETRIEVE SCHEDULE CONFIGURATION REMOVED NOTIFICATIONS - PULL POINT

Test Label: Retrieve Schedule Configuration Removed Notifications - Pull Point

Test Case ID: SCHEDULENOTIFICATIONS-2

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Configuration/Schedule/Removed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about schedule configuration removing 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 present wich is not filter out notification with topic **tns1:Configuration/Schedule/Removed**.
- Device supports Schedule Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Configuration/Schedule/Removed** notifications from the Device.
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:Configuration/Schedule/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/Schedule/Removed** OR **tns1:Configuration/Schedule//.** 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: schedules_notifications.configuration_schedule_removed

RETRIEVE SCHEDULE CONFIGURATION CHANGED NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Schedule Configuration Changed Notifications - Basic Notification

Test Case ID: SCHEDULENOTIFICATIONS-3

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Configuration/Schedule/Changed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about schedule configuration changes from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic **tns1:Configuration/Schedule/Changed**.
- Device supports Schedule Service.
- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Configuration/Schedule/Changed** notifications from the Device.
2. Device responses with code HTTP 200 OK and **SubscribeResponse** message.

Test Result:

PASS -

- Client **Subscribe** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **Subscribe** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **wsnt:Subscribe** AND
  - If it contains **wsnt: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/Schedule/Changed** AND

- If it contains **wsnt: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/Schedule/Changed** OR **tns1:Configuration/Schedule//.** OR **tns1:Configuration//.** in expression AND

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

FAIL -

- The Client failed PASS criteria.

Validated Feature List: schedules_notifications.configuration_schedule_changed_bn

RETRIEVE SCHEDULE CONFIGURATION REMOVED NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Schedule Configuration Removed Notifications - Basic Notification

Test Case ID: SCHEDULENOTIFICATIONS-4

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Configuration/Schedule/Removed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about schedule configuration removing from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic tns1:Configuration/Schedule/Removed.
- Device supports Schedule Service.
- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Configuration/Schedule/Removed** notifications from the Device.
2. Device responses with code HTTP 200 OK and **SubscribeResponse** message.

Test Result:

PASS -

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

- [S1] **soapenv:Body** element has child element **wsnt:Subscribe** AND
- If it contains **wsnt: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/Schedule/Removed** AND
- If it contains **wsnt: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/Schedule/Removed** OR **tns1:Configuration/Schedule//.** OR **tns1:Configuration//.** in expression AND

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

FAIL -

- The Client failed PASS criteria.

Validated Feature List: schedules_notifications.configuration_schedule_removed_bn

Get Access Profiles List Test Cases

Feature Level Normative Reference:

Validated Feature: get_access_profile_list

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client connects to Device to retrieve a complete list of Access Profiles.
2. Client is considered as supporting Get Access Profiles List if the following conditions are met:
   - Client is able to list available Access Profiles using **GetAccessProfileInfoList** operation OR **GetAccessProfileList** operation.
3. Client is considered as NOT supporting Get Access Profiles List if ANY of the following is TRUE:
   - No valid responses for **GetAccessProfileInfoList** request OR **GetAccessProfileList** request OR
   - **GetAccessProfileInfoList** request contains **tsc:StartReference** element value that was not recieved in **GetAccessProfileInfoList** response in **tsc:NextStartReference** element OR
   - **GetAccessProfileList** request contains **tsc:StartReference** element value that was not recieved in **GetAccessProfileList** response in **tsc:NextStartReference** element OR
   - Complete Access Profiles list was not received.

LISTING OF ACCESS PROFILES

Test Label: Get Access Profiles List - Listing of Access Profiles

Test Case ID: GETACCESSPROFILELIST-1

Profile A Normative Reference: Optional

Feature Under Test: Get Access Profiles List

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

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetAccessProfileList** operation present.
- Device supports Access Rules Service.

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

1. Client invokes **GetAccessProfileList** request message with skipped **tar:StartReference** element to retrieve first part of the list of all access profiles configured on the Device.
2. Device responses with code HTTP 200 OK and **GetAccessProfileListResponse** message.
3. If **GetAccessProfileListResponse** message contains **tar:NextStartReference** element Client invokes **GetAccessProfileList** request message with **tar:StartReference** element equal to value of **tar:NextStartReference** element to retrieve next part of the list of all access profiles configured on the Device.
4. Client repeats the previous step while **GetAccessProfileListResponse** message contains **tar:NextStartReference** element.

Test Result:

PASS -

- Client **GetAccessProfileList** request messages are valid according to XML Schemas listed in Namespaces AND
- First Client **GetAccessProfileList** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tar:GetAccessProfileList** AND
  - [S2] It does not contain **tar:StartReference** element AND
- If response on previous **GetAccessProfileList** request contains **tcr:NextStartReference** element each next Client **GetAccessProfileList** requests in Test Procedure fulfills the following requirements (else skip the checks):
  - [S3] **soapenv:Body** element has child element **tar:GetAccessProfileList** AND
  - [S4] It contains **tar:StartReference** element equal to **tar:NextStartReference** element from response on previous **GetAccessProfileList** request AND

- Device responses on the each **GetAccessProfileList** request in Test Procedure fulfills the following requirements:
  - [S5] It has HTTP 200 response code AND
  - [S6] **soapenv:Body** element has child element **tar:GetAccessProfileListResponse** AND
- The last in Test Procedure Device response on **GetAccessProfileList** request fulfills the following requirements:
  - [S7] It does not contain **tcr:NextStartReference** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_access_profile_list.get_access_profile_list

LISTING OF ACCESSPROFILE INFO

Test Label: Get Access Profiles List - Listing of Access Profile Info

Test Case ID: GETACCESSPROFILELIST-2

Profile A Normative Reference: Mandatory

Feature Under Test: Get Access Profile Info List

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

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **GetAccessProfileInfoList** operation present.
- Device supports Access Rules Service.

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

1. Client invokes **GetAccessProfileInfoList** request message with skipped **tar:StartReference** element to retrieve first part of the list of all access profiles configured on the Device.
2. Device responses with code HTTP 200 OK and **GetAccessProfileInfoListResponse** message.
3. If **GetAccessProfileInfoListResponse** message contains **tar:NextStartReference** element Client invokes **GetAccessProfileInfoList** request message with **tar:StartReference** element equal to value of **tar:NextStartReference** element to retrieve next part of the list of all access profiles configured on the Device.
4. Client repeats the previous step while **GetAccessProfileInfoListResponse** message contains **tar:NextStartReference** element.

Test Result:

PASS -

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

- First Client **GetAccessProfileInfoList** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tar:GetAccessProfileInfoList** AND
  - [S2] It does not contain **tar:StartReference** element AND
- If response on previous **GetAccessProfileInfoList** request contains **tcr:NextStartReference** element each next Client **GetAccessProfileInfoList** requests in Test Procedure fulfills the following requirements (else skip the checks):
  - [S3] **soapenv:Body** element has child element **tar:GetAccessProfileInfoList** AND
  - [S4] It contains **tar:StartReference** element equal to **tar:NextStartReference** element from response on previous **GetAccessProfileInfoList** request AND
- Device responses on the each **GetAccessProfileInfoList** request in Test Procedure fulfills the following requirements:
  - [S5] It has HTTP 200 response code AND
  - [S6] **soapenv:Body** element has child element **tar:GetAccessProfileInfoListResponse** AND
- The last in Test Procedure Device response on **GetAccessProfileInfoList** request fulfills the following requirements:
  - [S7] It does not contain **tcr:NextStartReference** element.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_access_profile_list.get_access_profile_info_list

Access Profile Configuration Notifications Test Cases

Feature Level Normative Reference:

Validated Feature: access_profiles_notifications

Profile A Requirement: Mandatory

Expected Scenarios Under Test:

1. Client subscribes to device messages using **CreatePullPointSubscription** operation OR **Subscribe** operation to get access profiles configuration notifications.
2. Client uses Pull Point event mechanism OR Basic Notification event mechanism (if Device supports Basic Notification event mechanism) to retrieve notification events from Device.
3. Client is considered as supporting Access Profile Configuration if the following conditions are met:
   - Client supports EventHandling_Pullpoint feature OR EventHandling_WS-BaseNotification feature AND
   - Client supports get_access_profile_list feature AND

- Client is able to retrieve notifications about access profile configuration change AND
- Client is able to retrieve notifications about access profile removing AND

4. Client is considered as NOT supporting Access Profile Configuration and State Notifications if ANY of the following is TRUE:
   - Client does not support EventHandling_Pullpoint feature AND EventHandling_WS-BaseNotification feature OR
   - Client does not support get_access_profile_list feature OR
   - Client is not able to retrieve notifications about access profile configuration change OR
   - Client is not able to retrieve notifications about access profile removing.

RETRIEVE ACCESS PROFILE CONFIGURATION CHANGED NOTIFICATIONS

Test Label: Retrieve Access Profile Configuration Changed Notifications

Test Case ID: ACCESSPROFILENOTIFICATIONS-1

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Configuration/AccessProfile/Changed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about access profile configuration changes 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 present wich is not filter out notification with topic **tns1:Configuration/AccessProfile/Changed**.
- Device supports Access Rules Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Configuration/AccessProfile/Changed** notifications from the Device.
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:Configuration/AccessProfile/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/AccessProfile/Changed** OR **tns1:Configuration/AccessProfile//.** 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: access_profiles_notifications.configuration_access_profile_changed

RETRIEVE ACCESS PROFILE CONFIGURATION REMOVED NOTIFICATIONS

Test Label: Retrieve Access Profile Configuration Removed Notifications

Test Case ID: ACCESSPROFILENOTIFICATIONS-2

Profile A Normative Reference: Mandatory

Feature Under Test: Receiving **tns1:Configuration/AccessProfile/Removed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about access profile configuration removing 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 present wich is not filter out notification with topic **tns1:Configuration/AccessProfile/Removed**.
- Device supports Access Rules Service.

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

1. Client invokes **CreatePullPointSubscription** request message to create subscribtion to retrieve at least **tns1:Configuration/AccessProfile/Removed** notifications from the Device.
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:Configuration/AccessProfile/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/AccessProfile/Removed** OR **tns1:Configuration/AccessProfile//.** 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: access_profiles_notifications.configuration_access_profile_removed

RETRIEVE ACCESS PROFILE CONFIGURATION CHANGED NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Access Profile Configuration Changed Notifications - Basic Notification

Test Case ID: ACCESSPROFILENOTIFICATIONS-3

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Configuration/AccessProfile/Changed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about access profile configuration changes from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic **tns1:Configuration/AccessProfile/Changed**.
- Device supports Access Rules Service.

- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Configuration/AccessProfile/Changed** notifications from the Device.

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

Test Result:

PASS -

- Client **Subscribe** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **Subscribe** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **wsnt:Subscribe** AND
  - If it contains **wsnt: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/AccessProfile/Changed** AND
  - If it contains **wsnt: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/AccessProfile/Changed** OR **tns1:Configuration/AccessProfile//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **Subscribe** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **wsnt:SubscribeResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: access_profiles_notifications.configuration_access_profile_changed_bn

RETRIEVE ACCESS PROFILE CONFIGURATION REMOVED NOTIFICATIONS - BASIC NOTIFICATION

Test Label: Retrieve Access Profile Configuration Removed Notifications - Basic Notification

Test Case ID: ACCESSPROFILENOTIFICATIONS-4

Profile A Normative Reference: None

Feature Under Test: Receiving **tns1:Configuration/AccessProfile/Removed** Notification

Test Purpose: To verify that Client is able to retrieve notifications about access profile configuration removing from Device using the Basic Notification event mechanism.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device with **Subscribe** operations present wich is not filter out notification with topic **tns1:Configuration/AccessProfile/Removed**.
- Device supports Access Rules Service.
- Device supports Basic Notification.

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

1. Client invokes **Subscribe** request message to create subscribtion to retrieve at least **tns1:Configuration/AccessProfile/Removed** notifications from the Device.
2. Device responses with code HTTP 200 OK and **SubscribeResponse** message.

Test Result:

PASS -

- Client **Subscribe** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **Subscribe** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **wsnt:Subscribe** 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/AccessProfile/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/AccessProfile/Removed** OR **tns1:Configuration/AccessProfile//.** OR **tns1:Configuration//.** in expression AND
- Device response on the **Subscribe** request fulfills the following requirements:
  - [S4] It has HTTP 200 response code AND
  - [S5] **soapenv:Body** element has child element **wsnt:SubscribeResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: access_profiles_notifications.configuration_access_profile_removed_bn

A. Revision History

December 07, 2016 Version 16.01

- General item (Test Overview) was added
- Minor updates in formatting, typos and terms
- Updates according review results (general changes): All test cases and use cases
- The following tests logic was updated to include logic for the case when all items were received in first GetXListResponse:
  - GETCREDENTIALLIST-1
  - GETCREDENTIALLIST-2
  - GETSCHEDULELIST-1
  - GETSCHEDULELIST-2
  - GETACCESSPROFILELIST-1
  - GETACCESSPROFILELIST-2

October 13, 2016 Version 15.10

- Initial version:

  General parts added

  Get Credentials List Test Cases added

  Get Credentials Details Test Cases added

  Credential Configuration and State Notifications Test Cases added

  Configure Credentials Test Cases

  Get Schedules List Test Cases added

  Schedules Configuration Notifications Test Cases added

  Get Access Profiles List Test Cases added

  Access Profiles Configuration Notifications Test Cases added

  Get Credential Capabilities added