ONVIF™

Profile Q Client Test Specification

Version 17.06

June 2017

REVISION HISTORY

Vers.	Date	Description
17.06	Jun 15, 2017	Links in Normative references section were updated.
16.07	Mar 14, 2016	www.onvif.org was removed from Copyright section.
16.01	Nov 23, 2015	General item (Test Owerview) was added Minor updates in formatting, typos and terms.
16.01	Sep 25, 2015	Initial version: General parts added Transition to Operational State Test Cases added

Table of Contents

1 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 Q features of a Client application e.g. Transition to Operational State. It also describes the test framework, test setup, prerequisites, test policies needed for the execution of the described test cases.

1.1 Scope

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

The principal intended purposes are:

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

1.2 Transition to Operational State

Transition to Operational State section specifies Client ability to transit an ONVIF Device from Factory Default State into Operational State.

2 Normative references

- ONVIF Conformance Process Specification:

  https://www.onvif.org/profiles/conformance/

- ONVIF Profile Policy:

  https://www.onvif.org/profiles/

- ONVIF Core Specifications:

  https://www.onvif.org/profiles/specifications/

- ONVIF Core Client Test Specification:

  https://www.onvif.org/profiles/conformance/client-test/

- ONVIF Profile Q Specification:

  https://www.onvif.org/profiles/profile-q/

- ISO/IEC Directives, Part 2, Annex H:

  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/]

- W3C Web Services Addressing 1.0 – Core:

  http://www.w3.org/TR/ws-addr-core/

3 Terms and Definitions

3.1 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].

3.2 Definitions

This section describes terms and definitions used in this document.

Profile	See ONVIF Profile Policy.
Profile Q	The Profile Q 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 contain 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.
Factory Default State	The state of the Profile Q device prior to setting an Administrator password. In this state, the device accepts any commands without authentication.
Operational State	The state of the Profile Q device after setting an Administrator password. The device requires an authentication according to the ONVIF default access policy to accept commands.

3.3 Abbreviations

This section describes abbreviations used in this document.

HTTP	Hyper Text Transport Protocol.

HTTPS	Hyper Text Transport Protocol over Secure Socket Layer.
IP	Internet Protocol.
IPv4	Internet Protocol version 4.
TCP	Transport Control Protocol.
UDP	User Datagram Protocol.
URI	Uniform Resource Identifier.
WSDL	Web Services Description Language.
WS-I BP 2.0	Web Services Interoperability Basic Profile version 2.0.
XML	eXtensible Markup Language.

3.4 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 3.1. 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
tas	http://www.onvif.org/ver10/advancedsecurity/wsdl	The namespace for the WSDL advanced security service
wsnt	http://docs.oasis-open.org/wsn/b-2	Schema namespace of the [WS-BaseNotification] specification.

4 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 Q is an ONVIF Client that can transit an ONVIF Device conformant to Profile Q into Operational State.

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.

4.1 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

4.1.1 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.

4.1.2 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.

4.1.3 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.

4.2 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 Q, the ONVIF Client shall follow the requirements of the conformance process. For details, please, see the latest ONVIF Conformance Process Specification.

4.3 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.

5 Transition to Operational State Test Cases

5.1 Feature Level Requirement:

Validated Feature: TransitionToOperationalState

Profile Q Requirement: Mandatory

5.2 Expected Scenarios Under Test:

1. A Client connects to a Device in Factory Default State to invoke its transition into Operational State.
2. The Client is considered as supporting Transition to Operational State if the following conditions are met:
   - The Client is able to invoke the Device transition into the Operational State by using EITHER **CreateUsers** OR **SetUser** operations.
3. The Client is considered as NOT supporting Transition to Operational State if ANY of the following is TRUE:
   - No valid response to **CreateUsers** request OR
   - No valid response to **SetUser** request AND
   - **SetUser** request does not contain user with **Username** value contained in **GetUsers** response.

5.3 TRANSITION TO OPERATIONAL STATE BY CREATEUSERS

Test Label: Transition to Operational State by Create User

Test Case ID: TRANSITIONTOOPERATIONALSTATE-1

Profile Q Normative Reference: Mandatory

Feature Under Test: Transition to Operational State

Test Purpose: To verify that a Client is able to invoke Device transition into Operational State using the **CreateUsers**.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device in Factory Default state with **CreateUsers** operation without any authentication which contains User with "Administrator" user level present.

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

1. Client invokes **CreateUsers** request message without any authentication and with non-empty password to create a new admin user.
2. Device responds with code HTTP 200 OK and **CreateUsersResponse** message.

Test Result:

PASS -

- Client **CreateUsers** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreateUsers** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tds:CreateUsers** AND
  - [S2] It does not contain Digest Authentication part AND
  - [S3] It does not contain WS-Username Token Authentication part AND
  - It contains **tds:User** element which fulfills the following requirements:
    - [S4] **tt:Username** element has non-empty string value AND
    - [S5] It contains **tt:Password** element AND
    - [S6] **tt:Password** element has non-empty string value AND
    - [S7] **tt:UserLevel** element value equals "Administrator" AND
- Device response to the **CreateUsers** request fulfills the following requirements:
  - [S8] It has HTTP 200 response code AND
  - [S9] **soapenv:Body** element has child element **tds:CreateUsersResponse**

FAIL -

- The Client failed PASS criteria.

Validated Feature List: transition_to_operational_state.create_users

5.4 TRANSITION TO OPERATIONAL STATE BY SET USER

Test Label: Transition to Operational State by Set User

Test Case ID: TRANSITIONTOOPERATIONALSTATE-2

Profile Q Normative Reference: Mandatory

Feature Under Test: Transition to Operational State

Test Purpose: To verify that a Client is able to invoke Device transition into Operational State using the **SetUser**.

Pre-Requisite:

- The Network Trace Capture files contains at least one Conversation between Client and Device in Factory Default state with **SetUser** operation without any authentication and with UserLevel is equal to "Administrator" present.

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

1. Client invokes **GetUsers** request message without any authentication to retrieve user list from Device.
2. Device responds with code HTTP 200 OK and **GetUsersResponse** message.
3. Client invokes **SetUser** request message without any authentication to modify the password of an existing admin user.
4. Device responds with code HTTP 200 OK and **SetUserResponse** message.

Test Result:

PASS -

- Client **SetUser** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **SetUser** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **tds:SetUser** AND
  - [S2] It does not contain Digest Authentication part AND
  - [S3] It does not contain WS-Username Token Authentication part AND
  - It contains **tds:User** element which fulfills the following requirements:

- [S4] **tt:Username** element has non-empty string value AND
- [S5] It contains **tt:Password** element AND
- [S6] **tt:Password** element has non-empty string value AND
- [S7] **tt:UserLevel** element value equals "Administrator" AND

- Device response to the **SetUser** request fulfills the following requirements:
  - [S8] It has HTTP 200 response code AND
  - [S9] **soapenv:Body** element has child element **tds:SetUserResponse**
- There is a Client **GetUsers** request message in Test Procedure fulfills the following requirements:
  - [S10] It is invoked for the same Device as the response for the **SetUser** request AND
  - [S11] It is invoked before the Client **SetUser** request AND
  - [S12] It does not contain digest authentication part AND
  - [S13] It does not contain WS-username token authentication part AND
- Device response to the **GetUsers** request fulfills the following requirements:
  - [S14] It has HTTP 200 response code AND
  - [S15] **soapenv:Body** element has child element **tds:GetUsersResponse**
  - [S16] It contains **tt:User** element which fulfills the following requirements:
    - [S17] **tt:Username** element value equals to **tt:Username** value from the **SetUser** request AND
    - [S18] **UserLevel** element value equals "Administrator".

FAIL -

- The Client failed PASS criteria.

Validated Feature List: transition_to_operational_state.set_user