ONVIF®

Access Policy Device Test Specification

Version 21.12

December 2021

Access Policy Device Test Spec

© 2021 ONVIF, Inc. All rights reserved.

Recipients of this document may copy, distribute, publish, or display this document so long as this copyright notice, license and disclaimer are retained with all copies of the document. No license is granted to modify this document.

THIS DOCUMENT IS PROVIDED "AS IS," AND THE CORPORATION AND ITS MEMBERS AND THEIR AFFILIATES, MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THIS DOCUMENT ARE SUITABLE FOR ANY PURPOSE; OR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

IN NO EVENT WILL THE CORPORATION OR ITS MEMBERS OR THEIR AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THIS DOCUMENT, WHETHER OR NOT (1) THE CORPORATION, MEMBERS OR THEIR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (2) SUCH DAMAGES WERE REASONABLY FORESEEABLE, AND ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THIS DOCUMENT. THE FOREGOING DISCLAIMER AND LIMITATION ON LIABILITY DO NOT APPLY TO, INVALIDATE, OR LIMIT REPRESENTATIONS AND WARRANTIES MADE BY THE MEMBERS AND THEIR RESPECTIVE AFFILIATES TO THE CORPORATION AND OTHER MEMBERS IN CERTAIN WRITTEN POLICIES OF THE CORPORATION.

REVISION HISTORY

Vers.	Date	Description
21.06	Jun 09, 2021	First Issue.
21.06	Jun 22, 2021	Update after Working Groupp review.
21.12	Oct 07, 2021	The following tests and annexes were moved to Access Policy Device Test Specification according to #2204: ACCESS_POLICY-1-1-2 Default access policy - Anonymous ACCESS_POLICY-1-1-3 Default access policy - User ACCESS_POLICY-1-1-4 Default access policy - Administrator and Anonymous ACCESS_POLICY-1-1-5 Default access policy - Administrator And User/Operator A.3 Create user with defined user level A.4 Get service capabilities
21.12	Oct 08, 2021	The following annexes were added according to #2233: A.5 Acceptable Faults The following tests were updated according to #2233: ACCESS_POLICY-1-1-1 ACCESS POLICY (ACCESS NOT ALLOWED) The following annexes were updated according to #2232: A.1 User Credentials File The following annexes were updated according to #2213: A.2 Access Policy File

Table of Contents

1 Introduction

Access control for ONVIF, including the ONVIF Default Access Policy, is described in the ONVIF Core Specification, section 5.9.2. User-based access control. The recommended access class for each service request is described in the ONVIF service specifications.

This test case has been created so that ONVIF members can test whether a device is correctly following an access policy, whether it is the default access policy or a proprietary access policy.

As the default access policy described in ONVIF Core Specification section 5.9.2.4 is not mandatory, the Default Access Policy Test Case is in Diagnostic mode only in the ONVIF Device Test Tool.

This test case is currently in beta stage and is provided as is, with no guarantees for its accuracy.

1.1 Scope

This ONVIF Access Policy Device Test Specification defines and regulates the testing procedure of the access policy for ONVIF conformant devices. Access policy testing is meant to be non-functional black box testing. The objective of this specification to provide test cases to test individual requirements of ONVIF devices according to ONVIF Access Policy Specification which is defined in [ONVIF Network Interface Specifications].

The principal intended purposes are:

- Provide self-assessment tool for implementations.
- Provide comprehensive test suite coverage for [ONVIF Network Interface Specifications].

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

- Product use cases and functional (performance and regression) testing.
- SOAP Implementation Interoperability test i.e. Web Service Interoperability Basic Profile version 2.0 (WS-I BP 2.0).
- Network protocol implementation, conformance tests for HTTP, HTTPS, RTP and RTSP protocols.
- Poor streaming performance test (audio/video distortions, missing audio/video frames, incorrect library synchronization etc.).

  Wi-Fi conformance test.

The set of ONVIF Test Specification will not cover the complete set of requirements as defined in [ONVIF Network Interface Specifications]; instead, it will cover its subset.

This ONVIF Access Policy Device Test Specification covers requirements for user-based access control, which is a functional block of [ONVIF Network Interface Specifications]. The following section gives a brief overview of each functional block and its scope.

1.2 Access Policy

Access Policy cases cover verification of user-based access control defined in [ONVIF Core Specification].

2 Normative references

- [ONVIF Conformance] ONVIF Conformance Process Specification:

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

- [ONVIF Profile Policy] ONVIF Profile Policy:

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

- [ONVIF Network Interface Specs] ONVIF Network Interface Specification documents:

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

- [ONVIF Core Specs] ONVIF Core Specification:

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

- [ONVIF Base Test] ONVIF Base Device Test Specification:

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

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

  http://www.iso.org/directives

- [ISO 16484-5] ISO 16484-5:2014-09 Annex P:

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

- [SOAP 1.2, Part 1] W3C SOAP 1.2, Part 1, Messaging Framework:

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

- [XML-Schema, Part 1] W3C XML Schema Part 1: Structures Second Edition:

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

- [XML-Schema, Part 2] W3C XML Schema Part 2: Datatypes Second Edition:

  http://www.w3.org/TR/xmlschema-2/

- [WS-Security] "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", OASIS Standard, February 2006.:

  http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

- [RFC 2396] "Uniform Resource Identifiers (URI): Generic Syntax", T. Berners-Lee, MIT/LCS, R. Fielding, U.C. Irvine, L. Masinter, Xerox Corporation, August 1998:

  https://www.ietf.org/rfc/rfc2396.txt

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.

ONVIF Device (DUT) 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.

ONVIF Device Test Tool ONVIF Device Test Tool that tests ONVIF Device implementation towards the ONVIF Test Specification set.

3.3 Abbreviations

This section describes abbreviations used in this document.

UI User Interface.

DUT Device Under Test.

4 Test Overview

This section describes about the test setup and prerequisites needed, and the test policies that should be followed for test case execution.

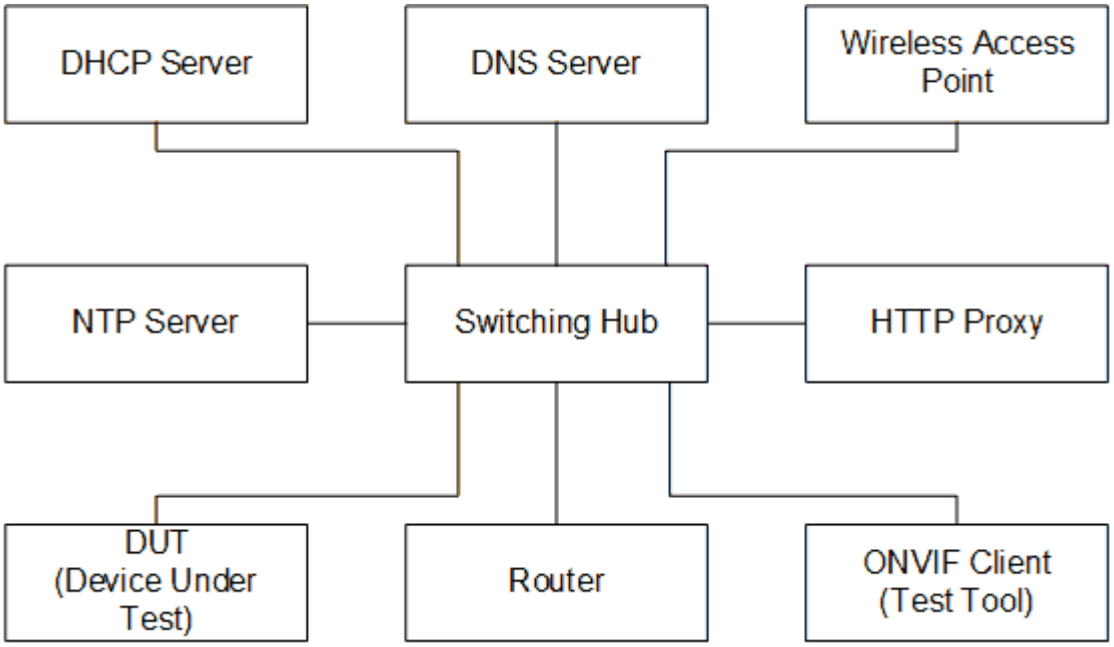
4.1 Test Setup

4.1.1 Network Configuration for an ONVIF Device

The generic test configuration for the execution of test cases defined in this document is as shown below (Figure 4.1).

Based on the individual test case requirements, most of the entities in the below setup may not be needed for the execution of those corresponding test cases.

Figure 4.1. Test Configuration for an ONVIF Device



DUT: ONVIF device to be tested. Hereafter, this is referred to as DUT (Device Under Test).

ONVIF Client (Test Tool): Tests are executed by this system, and it verifies the behavior of the DUT. It handles both expected and unexpected behavior.

HTTP Proxy: Provides facilitation in case of RTP and RTSP tunneling over HTTP.

Wireless Access Point: Provides wireless connectivity to the devices that support wireless connection.

DNS Server: Provides DNS related information to the connected devices.

DHCP Server: Provides IPv4 address to the connected devices.

NTP Server: Provides time synchronization between ONVIF Client and DUT.

Switching Hub: Provides network connectivity among all the test equipment in the test environment. All devices should be connected to the Switching Hub. When running multiple test instances in parallel on the same network, the Switching Hub should be configured to use filtering to avoid multicast traffic being flooded to all ports, because this may affect test stability.

Router: Provides router advertisements for IPv6 configuration.

4.2 Pre-requisites

The pre-requisites for executing the test cases described in this test specification are:

1. The ONVIF Device shall be configured with an IPv4 address.
2. The ONVIF Device shall be IP reachable in the test environment.
3. The ONVIF Device shall be able to be discovered by the Test Tool.
4. The ONVIF Device shall be configured with at least one user account from each available user group.

4.3 Test Policy

This section describes the test policies, specific to the test case execution of each functional block.

The ONVIF Device shall adhere to the test policies defined in this section.

4.3.1 Access Policy

The following tests are performed

- Negative test case ACCESS_POLICY-1-1-1 ACCESS POLICY (ACCESS NOT ALLOWED). This test case goal is checking that a DUT does not allow access for user level lower than the last allowed user level.
  - If Access Policy of a DUT is allowed access to a service request for Administrator only, then a DUT shall reject access for Operator user level.
  - If Access Policy of a DUT is allowed access to a service request for Administrator and Operator, then a DUT shall reject access for User user level.

- If Access Policy of a DUT is allowed access to a service request for Administrator, Operator, and User, then a DUT shall reject access for Anonymous.
- DTT expects HTTP error code 401 or env:Receiver/ter:ActionNotSupported SOAP fault message or env:Receiver/ter:ActionNotSupported/subcode SOAP fault message from a device.
- A device shall have full set of users in the User Credentials file in case Default Access Policy File is used.

Please, refer to Section 5 for Access Policy Test Cases.

5 Access Policy Test Cases

5.1 ACCESS POLICY (ACCESS NOT ALLOWED)

Test Case ID: ACCESS_POLICY-1-1-1

Specification Coverage: User-based access control (ONVIF Core Specification)

Feature Under Test: Access Policy

WSDL Reference: None.

Test Purpose: To verify that a DUT does not authorize service requests for users with prohibited security level.

Pre-requisite:

- Digest is supported by a DUT.
- If a DUT has custom User Credentials, then User Credentials file is provided by Test Operator using the Device Test Tool UI (please, see Annex Annex A.1).
- If a DUT has custom Access Policy, then Access Policy File is provided by Test Operator using the Device Test Tool UI (please, see Annex Annex A.2).
- Test operator chose which faults are treated as PASSED (please, see Annex Annex A.5).

Test Configuration: ONVIF Client and DUT

Test Procedure:

1. Start an ONVIF Client.
2. Start the DUT.
3. ONVIF Client validates Access Policy File and User Credentials consistency
   - 3.1. Set *userList* := User Credentials file from UI (see Annex Annex A.1).
   - 3.2. If Access Policy File is not provided in the Device Test Tool UI
     - 3.2.1. Set *accessPolicyFile* := Default Access Policy File (see Annex Annex A.2).
     - 3.2.2. If *userList* does not contain user with user level "User", FAIL the test and skip other steps.
     - 3.2.3. If *userList* does not contain user with user level "Operator", FAIL the test and skip other steps.

3.3. If Access Policy File is provided in the Device Test Tool UI

3.3.1. Set *accessPolicyFile* := Custom Access Policy File from UI (see Annex Annex A.2).

3.3.2. If *accessPolicyFile* contains at least one Request in AccessGroup with UserLevel="User" and *userList* does not contain user with user level "User", FAIL the test and skip other steps.

3.3.3. If *accessPolicyFile* contains contains at least one Request in AccessGroup with UserLevel="Operator" and *userList* does not contain user with user level "Operator", FAIL the test and skip other steps.

4. ONVIF Client sets users

4.1. Set *user* := User with UserLevel = "User" from *userList* if provided.

4.2. Set *operator* := User with UserLevel = "Operator" from *userList* if provided.

5. For each Request (*request*) from AccessGroup with UserLevel="User" from *accessPolicyFile* send the request with user level Anonymous (NOTE: only for services supported by ONVIF Client)

5.1. If DUT supports service that corresponds to Service.SpecificationName value of *request* in *accessPolicyFile*

5.1.1. ONVIF Client generates valid request structure with arbitrary values of parameters for command corresponds to *request*.

5.1.2. ONVIF Client invokes generated *request* without any credentials.

5.1.3. DUT responds with **HTTP error code 401** or with **env:Receiver/ter:ActionNotSupported** SOAP fault message or with **env:Receiver/ter:ActionNotSupported/subcode** SOAP fault message (see Annex Annex A.5).

6. For each Request (*request*) from AccessGroup with UserLevel="Operator" from *accessPolicyFile* send the request with user level User (NOTE: only for services supported by ONVIF Client)

6.1. If DUT supports service that corresponds to Service.SpecificationName of *request* in *accessPolicyFile*

6.1.1. ONVIF Client generates valid request structure with arbitrary values of parameters for command corresponds to *request*.

6.1.2. ONVIF Client invokes generated *request* with credentials of *user.* .

6.1.3. DUT responds with **HTTP error code 401** or with **env:Receiver/ter:ActionNotSupported** SOAP fault message or with **env:Receiver/ter:ActionNotSupported/subcode** SOAP fault message (see Annex Annex A.5).

7. For each Request (*request*) from AccessGroup with UserLevel="Administrator" from *accessPolicyFile* send the request with user level Operator (NOTE: only for services supported by ONVIF Client)

7.1. If DUT supports service that corresponds to Service.SpecificationName of *request* in *accessPolicyFile*

7.1.1. ONVIF Client generates valid request structure with arbitrary values of parameters for command corresponds to *request*.

7.1.2. ONVIF Client invokes generated *request* with credentials of *operator.* .

7.1.3. DUT responds with **HTTP error code 401** or with **env:Receiver/ter:ActionNotSupported** SOAP fault message or with **env:Receiver/ter:ActionNotSupported/subcode** SOAP fault message (see Annex Annex A.5).

Test Result:

PASS –

- DUT passes all assertions.

FAIL –

- The DUT did not send either HTTP error code 401 or env:Receiver/ter:ActionNotSupported SOAP fault message.

5.2 Default access policy - Anonymous

Test Case ID: ACCESS_POLICY-1-1-2

Specification Coverage: Default access policy

Feature Under Test: GetServices, GetServiceCapabilities, GetHostname, GetSystemDateAndTime

WSDL Reference: devicemgmt.wsdl

Test Purpose: To verify that operations in the PRE_AUTH access class can be accessed without authentication being required.

Pre-Requisite: GetServices command is supported by the DUT. Default Access Policy is supported by the DUT as indicated by the Security.DefaultAccessPolicy capability. HTTP Digest Authentication is supported by the DUT as indicated by the Security.HttpDigest capability. Default Access Policy is not modified.

Test Configuration: ONVIF Client and DUT

Test Sequence:

1. Start an ONVIF Client.
2. Start the DUT.
3. ONVIF client invokes **GetServices** for Device service without any authentication with parameters
   - IncludeCapability := false
4. The DUT responds with **GetServicesResponse** message with parameters
   - Service list
5. ONVIF client invokes **GetServiceCapabilities** for Device Service without any authentication.
6. The DUT responds with **GetServiceCapabilitiesResponse** message with parameters
   - Capabilities
7. ONVIF client invokes **GetHostname** without any authentication.
8. The DUT responds with **GetHostnameResponse** message with parameters
   - HostnameInformation
9. ONVIF client invokes **GetSystemDateAndTime** without any authentication.
10. The DUT responds with **GetSystemDateAndTimeResponse** message with parameters
    - SystemDateAndTime

Test Result:

PASS –

- The DUT passed all assertions.

FAIL –

- The DUT did not allow Anonymous access to the **GetServices** command.
- The DUT did not allow Anonymous access to the **GetServiceCapabilities** command.
- The DUT did not allow Anonymous access to the **GetHostname** command.
- The DUT did not allow Anonymous access to the **GetSystemDateAndTime** command.
- The DUT did not send **GetServicesResponse** message.
- The DUT did not send **GetServiceCapabilitiesResponse** message.
- The DUT did not send **GetHostnameResponse** message.
- The DUT did not send **GetSystemDateAndTimeResponse** message.

5.3 Default access policy - User

Test Case ID:ACCESS_POLICY-1-1-3

Specification Coverage: Default access policy

Feature Under Test: GetNTP, GetNetworkInterfaces, GetScopes, GetDiscoveryMode, GetEventProperties

WSDL Reference: devicemgmt.wsdl

Test Purpose: To verify that operations in the READ_SYSTEM and READ_MEDIA access classes can be accessed with authentication level User.

Pre-Requisite: GetServices command is supported by the DUT. Event Service was received from the DUT. Default Access Policy is supported by the DUT as indicated by the Security.DefaultAccessPolicy capability. HTTP Digest Authentication is supported by the DUT as indicated by the Security.HttpDigest capability. Maximum Username Length is supported by the DUT as indicated by the Capabilities.Security.MaxUsernameLength, Maximum Password Length is supported by the DUT as indicated by the Capabilities.Security.MaxPasswordLength. Default Access Policy is not modified.

Test Configuration: ONVIF Client and DUT

Test Sequence:

1. Start an ONVIF Client.

2. Start the DUT.
3. Set the following:
   - *userLevel* := User
4. ONVIF Client generates creates user with predefined user level (in *userLevel*) and user login (out *userLogin*) and password (out *password*) by following the procedure mentioned in Annex A.3.
5. If the DUT supports NTP as indicated by Network.NTP capability:
   5.1. ONVIF client invokes **GetNTP** without any authentication.
   5.2. The DUT responds with **HTTP 401 Unauthorized** error.
   5.3. ONVIF client invokes **GetNTP** with user with the user level User credantials (*userLogin* and *password*).
   5.4. The DUT responds with **GetNTPResponse** message with parameters
      - NTPInformation
6. ONVIF client invokes **GetNetworkInterfaces** without any authentication.
7. The DUT responds with **HTTP 401 Unauthorized** error.
8. ONVIF client invokes **GetNetworkInterfaces** with user with the user level User credantials (userLogin and password).
9. The DUT responds with **GetNetworkInterfacesResponse** message with parameters
   - NetworkInterfaces list
10. ONVIF client invokes **GetScopes** without any authentication.
11. The DUT responds with **HTTP 401 Unauthorized** error.
12. ONVIF client invokes **GetScopes** with user with the user level User credantials (*userLogin* and *password*).
13. The DUT responds with GetScopesResponse message with parameters
    - Scopes list
14. ONVIF client invokes **GetDiscoveryMode** without any authentication.
15. The DUT responds with **HTTP 401 Unauthorized** error.

16. ONVIF client invokes **GetDiscoveryMode** with user with the user level User credantials (*userLogin* and *password*).
17. The DUT responds with **GetDiscoveryModeResponse** message with parameters
    - DiscoveryMode
18. ONVIF client invokes **GetEventProperties** without any authentication.
19. The DUT responds with **HTTP 401 Unauthorized** error.
20. ONVIF client invokes **GetEventProperties** with user with the user level User credantials (*userLogin* and *password*).
21. The DUT responds with **GetEventPropertiesResponse** message with parameters
    - TopicNamespaceLocation list
    - FixedTopicSet
    - TopicSet
    - TopicExpressionDialect list
    - MessageContentFilterDialect list
    - ProducerPropertiesFilterDialect list
    - MessageContentSchemaLocation list
    - Other additional fields if any

Test Result:

PASS –

- The DUT passed all assertions.

FAIL –

- The DUT allow Anonymous access to the **GetNTP** command.
- The DUT allow Anonymous access to the **GetNetworkInterfaces** command.
- The DUT allow Anonymous access to the **GetScopes** command.
- The DUT allow Anonymous access to the **GetDiscoveryMode** command.
- The DUT allow Anonymous access to the **GetEventProperties** command.

- The DUT did not allow user with the user level User access to the **GetNTP** command.
- The DUT did not allow user with the user level User access to the **GetNetworkInterfaces** command.
- The DUT did not allow user with the user level User access to the **GetScopes** command.
- The DUT did not allow user with the user level User access to the **GetDiscoveryMode** command.
- The DUT did not allow user with the user level User access to the **GetEventProperties** command.
- The DUT did not send **GetNTPResponse** message.
- The DUT did not send **GetNetworkInterfacesResponse** message.
- The DUT did not send **GetScopesResponse** message.
- The DUT did not send **GetDiscoveryModeResponse** message.
- The DUT did not send **GetEventPropertiesResponse** message.

5.4 Default access policy - Administrator and Anonymous

Test Case ID: ACCESS_POLICY-1-1-4

Specification Coverage: Default access policy

Feature Under Test: SetScopes, SetDiscoveryMode, GetAccessPolicy, CreateUsers, SetSystemDateAndTime

WSDL Reference: devicemgmt.wsdl

Test Purpose: To verify that operations in the UNRECOVERABLE, WRITE_SYSTEM and READ_SYSTEM_SECRET access classes can notbe accessed without authentication level Administrator.

Pre-Requisite: GetServices command is supported by the DUT. Default Access Policy is supported by the DUT as indicated by the Security.DefaultAccessPolicy capability. HTTP Digest Authentication is supported by the DUT as indicated by the Security.HttpDigest capability. Default Access Policy is not modified.

Test Configuration: ONVIF Client and DUT

Test Sequence:

1. Start an ONVIF Client.
2. Start the DUT.
3. ONVIF Client gets the service capabilities (out cap) by following the procedure mentioned in Annex A.4
4. ONVIF client invokes **SetScopes** without any authentication with parameters
   - Scopes[0] := "onvif://www.onvif.org/location/test"
5. The DUT responds with **HTTP 401 Unauthorized** error.
6. ONVIF client invokes **SetDiscoveryMode** without any authentication with parameters
   - DiscoveryMode := Discoverable
7. The DUT responds with **HTTP 401 Unauthorized** error
8. If cap.Security contains AccessPolicyConfig and cap.Security.AccessPolicyConfig equals to true:
   8.1. ONVIF client invokes **GetAccessPolicy** without any authentication.
   8.2. The DUT responds with **HTTP 401 Unauthorized** error.
9. ONVIF client invokes **CreateUsers** without any authentication with parameters.
   - User[0].Username := "Test"
   - User[0].Password := "Test"
   - User[0].UserLevel := Administrator
   - Extension skipped
10. The DUT responds with **HTTP 401 Unauthorized** error.
11. ONVIF client invokes **SetSystemDateAndTime** without any authentication with parameters
    - DateTimeType := NTP
    - DaylightSavings := true
    - TimeZone skipped
    - UTCDateTime skipped
12. The DUT responds with **HTTP 401 Unauthorized** error.

Test Result:

PASS –

- The DUT passed all assertions.

FAIL –

- The DUT allowed Anonymous access to the **SetScopes** command.
- The DUT allowed Anonymous access to the **SetDiscoveryMode** command.
- The DUT allowed Anonymous access to the **GetAccessPolicy** command.
- The DUT allowed Anonymous access to the **CreateUsers** command.
- The DUT allowed Anonymous access to the **SetSystemDateAndTime** command.

Note: ONVIF client uses password values from Management tab for CreateUsers and StUser operations if 'Provide own passwords' is active on Management tab.

5.5 Default access policy - Administrator And User/Operator

Test Case ID: ACCESS_POLICY-1-1-5

Specification Coverage: Default access policy

Feature Under Test: SetScopes, SetDiscoveryMode, GetAccessPolicy, CreateUsers, SetSystemDateAndTime

WSDL Reference: devicemgmt.wsdl

Test Purpose: To verify that operations in the UNRECOVERABLE, WRITE_SYSTEM and READ_SYSTEM_SECRET access classes can not be accessed without authentication level Administrator.

Pre-Requisite: GetServices command is supported by the DUT. Default Access Policy is supported by the DUT as indicated by the Security.DefaultAccessPolicy capability. HTTP Digest Authentication is supported by the DUT as indicated by the Security.HttpDigest capability. Maximum Username Length is supported by the DUT as indicated by the Capabilities.Security.MaxUsernameLength, Maximum Password Length is supported by the DUT as indicated by the Capabilities.Security.Max PasswordLength.Default Access Policy is not modified.

Test Configuration: ONVIF Client and DUT

Test Sequence:

1. Start an ONVIF Client.
2. Start the DUT.
3. Set the following:
   - *userLevelUser* := User
   - *userLevelOperator*:= Operator
4. ONVIF Client generates creates user with predefined user level (in *userLevelUser*) and user login (out *userLoginUser*) and password (out *passwordUser*) by following the procedure mentioned in Annex A.3.
   - Scopes[0] := "onvif://www.onvif.org/location/test"
5. ONVIF Client gets the service capabilities (out cap) by following the procedure mentioned in Annex A.4.
6. ONVIF client invokes **SetScopes** with user with the user level User credantials (*userLoginUser* and *passwordUser*) with parameters
   - Scopes[0] := "onvif://www.onvif.org/location/test"
7. The DUT responds with **HTTP 401 Unauthorized** error
8. ONVIF client invokes **SetDiscoveryMode** with user with the user level User credantials (*userLoginUser* and *passwordUser*) with parameters
   - DiscoveryMode := Discoverable
9. The DUT responds with **HTTP 401 Unauthorized** error.
10. If *cap*.Security contains AccessPolicyConfig and *cap*.Security.AccessPolicyConfig equals to true:
    10.1. ONVIF client invokes **GetAccessPolicy** with user with the user level User credantials (*userLoginUser* and *passwordUser*).
    10.2. The DUT responds with **HTTP 401 Unauthorized** error.
11. ONVIF client invokes **CreateUsers** with user with the user level User credantials (*userLoginUser* and *passwordUser*).
    - User[0].Username := "Test"
    - User[0].Password := "Test"

- User[0].UserLevel := Administrator
- Extension skipped

12. The DUT responds with **HTTP 401 Unauthorized** error.
13. ONVIF client invokes **SetSystemDateAndTime** with user with the user level User credantials (*userLoginUser* and *passwordUser*).
    - DateTimeType := NTP
    - DaylightSavings := true
    - TimeZone skipped
    - UTCDateTime skipped
14. The DUT responds with **HTTP 401 Unauthorized** error.
15. ONVIF Client generates creates user with predefined user level (in userLevelOperator) and user login (out userLoginOperator) and password (out passwordOperator) by following the procedure mentioned in Annex A.3.
16. ONVIF client invokes **SetScopes** with user with the user level Operator credantials (*userLoginOperator* and *passwordOperator*) with parameters
    - DiscoveryMode := Discoverable
17. The DUT responds with **HTTP 401 Unauthorized** error.
18. ONVIF client invokes **SetDiscoveryMode** with user with the user level Operator credantials (*userLoginOperator* and *passwordOperator*) with parameters
    - DiscoveryMode := Discoverable
19. The DUT responds with **HTTP 401 Unauthorized** error.
20. If *cap*.Security contains AccessPolicyConfig and *cap*.Security.AccessPolicyConfig equals to true:
    20.1. ONVIF client invokes **GetAccessPolicy** with user with the user level User credantials (*userLoginUser* and *passwordUser*).
    20.2. The DUT responds with **HTTP 401 Unauthorized** error.
21. ONVIF client invokes **CreateUsers** with user with the user level User credantials (*userLoginUser* and *passwordUser*).

- User[0].Username := "Test"
- User[0].Password := "Test"
- User[0].UserLevel := Administrator
- Extension skipped

22. The DUT responds with **HTTP 401 Unauthorized** error.
23. ONVIF client invokes **SetSystemDateAndTime** with user with the user level User credantials (*userLoginUser* and *passwordUser*).
    - DateTimeType := NTP
    - DaylightSavings := true
    - TimeZone skipped
    - UTCDateTime skipped
24. The DUT responds with **HTTP 401 Unauthorized** error.

Test Result:

PASS –

- The DUT passed all assertions.

FAIL –

- The DUT allowed User access to the **SetScopes** command.
- The DUT allowed User access to the **SetDiscoveryMode** command.
- The DUT allowed User access to the **GetAccessPolicy** command.
- The DUT allowed User access to the **CreateUsers** command.
- The DUT allowed User access to the **SetSystemDateAndTime** command.
- The DUT allowed Operator access to the **SetScopes** command.
- The DUT allowed Operator access to the **SetDiscoveryMode** command.
- The DUT allowed Operator access to the **GetAccessPolicy** command.
- The DUT allowed Operator access to the **CreateUsers** command.

- The DUT allowed Operator access to the **SetSystemDateAndTime** command.

Note: ONVIF client uses password values from Management tab for CreateUsers and StUser operations if 'Provide own passwords' is active on Management tab.

Annex A Helper Procedures and Additional Notes

A.1 User Credentials File

The Device Test Tool uses the User Credentials File in ACCESS_POLICY-1-1-1 ACCESS POLICY (ACCESS NOT ALLOWED) test case.

This is a file that contains the username and password for two users that have user levels Operator and User respectively.

There are two options for the User Credentials File: **Default User Credentials File** and **Custom User Credentials File**.

1. Default User Credentials File:
   - It is an internal file provided with the Device Test Tool.
   - By default (if User Credentials File is not provided in the Device Test Tool UI), the ONVIF Client uses this Default User Credentials File.
   - Test operator shall create users on the Device Under Test with username/password specified in the Default User Credentials File.
2. Custom User Credentials File:
   - How to create Custom User Credentials File:
     - Get Default User Credentials File in the folder ONVIF Test Tool is installed to.
     - Modify User Credentials Policy File with username/password of users that already exist on the Device Under Test.
     - Provide modified file in the Device Test Tool UI.

Here is template of User Credentials File.

```
<?xml version="1.0"?>
<UserCredentialsDefinition xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xm
    <AccessLevels>
        <AccessLevel Name="Operator" Username="operator" Password="op_password"/>
        <AccessLevel Name="User" Username="user" Password="user_password"/>
    </AccessLevels>
</UserCredentialsDefinition>
```

A.2 Access Policy File

The Device Test Tool uses the Access Policy File in ACCESS_POLICY-1-1-1 ACCESS POLICY (ACCESS NOT ALLOWED) test case.

There are two options for the Access Policy File: **Default Access Policy File** and **Custom Access Policy File**.

1. Default Access Policy File:
   - It is an internal file provided with the Device Test Tool. It corresponds to Default Access Policy (defined in the Table 6 Default Access Policy Definition in ONVIF Core Specification).
   - By default (if Access Policy File is not provided in the Device Test Tool UI), the ONVIF Client uses this Default Access Policy File.
   - If a DUT Access Policy is the same as defined in the Table 6 Default Access Policy Definition of ONVIF Core Specification, test operator does not have to do anything with Access Policy File.
2. Custom Access Policy File:
   - If a DUT Access Policy differs from defined in the Table 6 Default Access Policy Definition of ONVIF Core Specification, test operator shall provide Custom Access Policy File in the Device Test Tool UI.
   - How to create Custom Access Policy File:
     - Get Default Access Policy File in the folder ONVIF Test Tool is installed to.
     - Modify Default Access Policy File with custom access policy.
     - Provide modified file in the Device Test Tool UI.

Description of Access Policy File structure:

- AccessGroup with UserLevel="Anonymous" contains set of requests that allow access for the following users levels: anonymous access and all user levels ("User", "Operator", "Administrator").
- AccessGroup with UserLevel="User" contains set of requests that allow access for the following users levels: "User", "Operator", "Administrator". Anonymous access is not allowed.

- AccessGroup with UserLevel="Operator" contains set of requests that allow access for the following users levels: "Operator", "Administrator". Anonymous access and access for "User" user level are not allowed.
- AccessGroup with UserLevel="Administrator" contains set of requests that allow access for "Administrator" user level only. Anonymous access and access for "User" and "Operator" user levels are not allowed.
- Service.@SpecificationName attribute has the name of specification where service operation is coming from as value.

Here is template of Access Policy File.

```
<?xml version="1.0"?>
<AccessPolicyDefinition xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns
  <AccessGroups>
    <AccessGroup UserLevel="Administrator">
      <Services>
        <Service SpecificationName="AccessControl">
          <Requests>
            <Request Name="CreateAccessPoint" />
            <Request Name="SetAccessPoint" />
            <Request Name="ModifyAccessPoint" />
            <Request Name="DeleteAccessPoint" />
            <Request Name="CreateArea" />
            <Request Name="SetArea" />
            <Request Name="ModifyArea" />
            <Request Name="DeleteArea" />
          </Requests>
        </Service>
        <Service SpecificationName="AccessRules">
          <Requests>
            <Request Name="CreateAccessProfile" />
            <Request Name="SetAccessProfile" />
            <Request Name="ModifyAccessProfile" />
            <Request Name="DeleteAccessProfile" />
          </Requests>
        </Service>
        <Service SpecificationName="ActionEngine">
          <Requests>
```

```
        <Request Name="CreateActions" />
        <Request Name="ModifyActions" />
        <Request Name="DeleteActions" />
        <Request Name="CreateActionTriggers" />
        <Request Name="ModifyActionTriggers" />
        <Request Name="DeleteActionTriggers" />
      </Requests>
    </Service>
    <Service SpecificationName="AnalyticsEngine">
      <Requests>
        <Request Name="DeleteAnalyticsModules" />
      </Requests>
    </Service>
    <Service SpecificationName="ApplicationManagement">
      <Requests>
        <Request Name="Uninstall" />
        <Request Name="Activate" />
        <Request Name="Deactivate" />
        <Request Name="GetInstalledApps" />
        <Request Name="GetAppsInfo" />
        <Request Name="InstallLicense" />
      </Requests>
    </Service>
    <Service SpecificationName="AuthenticationBehavior">
      <Requests>
        <Request Name="CreateAuthenticationProfile" />
        <Request Name="SetAuthenticationProfile" />
        <Request Name="ModifyAuthenticationProfile" />
        <Request Name="DeleteAuthenticationProfile" />
        <Request Name="CreateSecurityLevel" />
        <Request Name="SetSecurityLevel" />
        <Request Name="ModifySecurityLevel" />
        <Request Name="DeleteSecurityLevel" />
      </Requests>
    </Service>
    <Service SpecificationName="Core">
      <Requests>
        <Request Name="SetHostname" />
        <Request Name="SetHostnameFromDHCP" />
        <Request Name="SetDNS" />
```

```
            <Request Name="SetNTP" />
            <Request Name="SetDynamicDNS" />
            <Request Name="SetNetworkInterfaces" />
            <Request Name="SetNetworkProtocols" />
            <Request Name="SetNetworkDefaultGateway" />
            <Request Name="SetZeroConfiguration" />
            <Request Name="SetIPAddressFilter" />
            <Request Name="AddIPAddressFilter" />
            <Request Name="RemoveIPAddressFilter" />
            <Request Name="GetSystemBackup" />
            <Request Name="RestoreSystem" />
            <Request Name="StartSystemRestore" />
            <Request Name="SetSystemDateAndTime" />
            <Request Name="SetSystemFactoryDefault" />
            <Request Name="UpgradeSystemFirmware" />
            <Request Name="StartFirmwareUpgrade" />
            <Request Name="GetSystemLog" />
            <Request Name="GetSystemSupportInformation" />
            <Request Name="SystemReboot" />
            <Request Name="SetScopes" />
            <Request Name="AddScopes" />
            <Request Name="RemoveScopes" />
            <Request Name="SetDiscoveryMode" />
            <Request Name="SetGeoLocation" />
            <Request Name="DeleteGeoLocation" />
            <Request Name="GetAccessPolicy" />
            <Request Name="SetAccessPolicy" />
            <Request Name="GetUsers" />
            <Request Name="CreateUsers" />
            <Request Name="DeleteUsers" />
            <Request Name="SetUser" />
            <Request Name="SetRemoteUser" />
            <Request Name="SetPasswordComplexityConfiguration" />
            <Request Name="SetPasswordHistoryConfiguration" />
            <Request Name="SetAuthFailureWarningConfiguration" />
            <Request Name="AddEventBroker" />
            <Request Name="DeleteEventBroker" />
          </Requests>
        </Service>
        <Service SpecificationName="Credential">
```

```
      <Requests>
        <Request Name="GetCredentialInfoList" />
        <Request Name="GetCredentials" />
        <Request Name="GetCredentialList" />
        <Request Name="CreateCredential" />
        <Request Name="SetCredential" />
        <Request Name="ModifyCredential" />
        <Request Name="DeleteCredential" />
        <Request Name="GetCredentialIdentifiers" />
        <Request Name="SetCredentialIdentifier" />
        <Request Name="DeleteCredentialIdentifier" />
        <Request Name="GetWhitelist" />
        <Request Name="AddToWhitelist" />
        <Request Name="RemoveFromWhitelist" />
        <Request Name="DeleteWhitelist" />
        <Request Name="GetBlacklist" />
        <Request Name="AddToBlacklist" />
        <Request Name="RemoveFromBlacklist" />
        <Request Name="DeleteBlacklist" />
      </Requests>
    </Service>
    <Service SpecificationName="DeviceIO">
      <Requests>
        <Request Name="GetVideoOutputConfigurationOptions" />
      </Requests>
    </Service>
    <Service SpecificationName="DoorControl">
      <Requests>
        <Request Name="CreateDoor" />
        <Request Name="SetDoor" />
        <Request Name="ModifyDoor" />
        <Request Name="DeleteDoor" />
      </Requests>
    </Service>
    <Service SpecificationName="Imaging">
      <Requests>
        <Request Name="GetImagingSettings" />
        <Request Name="GetOptions" />
      </Requests>
    </Service>
```

```
<Service SpecificationName="Media">
  <Requests>
    <Request Name="SetVideoSourceMode" />
  </Requests>
</Service>
<Service SpecificationName="Media2">
  <Requests>
    <Request Name="SetVideoSourceMode" />
  </Requests>
</Service>
<Service SpecificationName="Provisioning">
  <Requests>
    <Request Name="PanMove" />
    <Request Name="TiltMove" />
    <Request Name="ZoomMove" />
    <Request Name="RollMove" />
    <Request Name="FocusMove" />
    <Request Name="Stop" />
  </Requests>
</Service>
<Service SpecificationName="Receiver">
  <Requests>
    <Request Name="GetReceivers" />
    <Request Name="GetReceiver" />
    <Request Name="GetReceiverState" />
  </Requests>
</Service>
<Service SpecificationName="RecordingSearch">
  <Requests>
    <Request Name="EndSearch" />
  </Requests>
</Service>
<Service SpecificationName="Schedule">
  <Requests>
    <Request Name="CreateSchedule" />
    <Request Name="SetSchedule" />
    <Request Name="ModifySchedule" />
    <Request Name="DeleteSchedule" />
    <Request Name="CreateSpecialDayGroup" />
    <Request Name="SetSpecialDayGroup" />
```

```
        <Request Name="ModifySpecialDayGroup" />
        <Request Name="DeleteSpecialDayGroup" />
      </Requests>
    </Service>
    <Service SpecificationName="Security">
      <Requests>
        <Request Name="UploadPassphrase" />
        <Request Name="GetAllPassphrases" />
        <Request Name="DeletePassphrase" />
        <Request Name="CreateRSAKeyPair" />
        <Request Name="UploadKeyPairInPKCS8" />
        <Request Name="GetKeyStatus" />
        <Request Name="GetPrivateKeyStatus" />
        <Request Name="GetAllKeys" />
        <Request Name="DeleteKey" />
        <Request Name="CreateSelfSignedCertificate" />
        <Request Name="UploadCertificate" />
        <Request Name="UploadCertificateWithPrivateKeyInPKCS12" />
        <Request Name="GetCertificate" />
        <Request Name="GetAllCertificates" />
        <Request Name="DeleteCertificate" />
        <Request Name="CreateCertificationPath" />
        <Request Name="GetCertificationPath" />
        <Request Name="GetAllCertificationPaths" />
        <Request Name="DeleteCertificationPath" />
        <Request Name="UploadCRL" />
        <Request Name="GetCRL" />
        <Request Name="GetAllCRLs" />
        <Request Name="DeleteCRL" />
        <Request Name="CreateCertPathValidationPolicy" />
        <Request Name="GetCertPathValidationPolicy" />
        <Request Name="GetAllCertPathValidationPolicies" />
        <Request Name="DeleteCertPathValidationPolicy" />
        <Request Name="AddServerCertificateAssignment" />
        <Request Name="RemoveServerCertificateAssignment" />
        <Request Name="ReplaceServerCertificateAssignment" />
        <Request Name="GetAssignedServerCertificates" />
        <Request Name="SetClientAuthenticationRequired" />
        <Request Name="SetCnMapsToUser" />
        <Request Name="AddCertPathValidationPolicyAssignment" />
```

```
            <Request Name="RemoveCertPathValidationPolicyAssignment" />
            <Request Name="ReplaceCertPathValidationPolicyAssignment" />
            <Request Name="GetAssignedCertPathValidationPolicies" />
            <Request Name="SetEnabledTLSVersions" />
            <Request Name="AddDot1XConfiguration" />
            <Request Name="GetAllDot1XConfigurations" />
            <Request Name="GetDot1XConfiguration" />
            <Request Name="DeleteDot1XConfiguration" />
            <Request Name="SetNetworkInterfaceDot1XConfiguration" />
            <Request Name="GetNetworkInterfaceDot1XConfiguration" />
            <Request Name="DeleteNetworkInterfaceDot1XConfiguration" />
          </Requests>
        </Service>
      </Services>
    </AccessGroup>
    <AccessGroup UserLevel="Operator">
      <Services>
        <Service SpecificationName="AccessControl">
          <Requests>
            <Request Name="SetAccessPointAuthenticationProfile" />
            <Request Name="DeleteAccessPointAuthenticationProfile" />
            <Request Name="GetAccessPointState" />
            <Request Name="EnableAccessPoint" />
            <Request Name="DisableAccessPoint" />
            <Request Name="ExternalAuthorization" />
            <Request Name="Feedback" />
          </Requests>
        </Service>
        <Service SpecificationName="AnalyticsEngine">
          <Requests>
            <Request Name="CreateRules" />
            <Request Name="ModifyRules" />
            <Request Name="DeleteRules" />
            <Request Name="CreateAnalyticsModules" />
            <Request Name="ModifyAnalyticsModules" />
          </Requests>
        </Service>
        <Service SpecificationName="Core">
          <Requests>
            <Request Name="SetRelayOutputSettings" />
```

```
        <Request Name="SetRelayOutputState" />
        <Request Name="SendAuxiliaryCommand" />
        <Request Name="CreateStorageConfiguration" />
        <Request Name="SetStorageConfiguration" />
        <Request Name="DeleteStorageConfiguration" />
      </Requests>
    </Service>
    <Service SpecificationName="Credential">
      <Requests>
        <Request Name="GetCredentialState" />
        <Request Name="EnableCredential" />
        <Request Name="DisableCredential" />
        <Request Name="ResetAntipassbackViolation" />
        <Request Name="SetCredentialAccessProfiles" />
        <Request Name="DeleteCredentialAccessProfiles" />
      </Requests>
    </Service>
    <Service SpecificationName="DeviceIO">
      <Requests>
        <Request Name="SetVideoOutputConfiguration" />
        <Request Name="SetRelayOutputSettings" />
        <Request Name="SetRelayOutputState" />
        <Request Name="SetDigitalInputConfigurations" />
        <Request Name="SetSerialPortConfiguration" />
        <Request Name="SendReceiveSerialCommand" />
      </Requests>
    </Service>
    <Service SpecificationName="Display">
      <Requests>
        <Request Name="SetPaneConfigurations" />
        <Request Name="SetPaneConfiguration" />
        <Request Name="CreatePaneConfiguration" />
        <Request Name="DeletePaneConfiguration" />
        <Request Name="SetLayout" />
      </Requests>
    </Service>
    <Service SpecificationName="DoorControl">
      <Requests>
        <Request Name="AccessDoor" />
        <Request Name="LockDoor" />
```

```
        <Request Name="UnlockDoor" />
        <Request Name="BlockDoor" />
        <Request Name="LockDownDoor" />
        <Request Name="LockDownReleaseDoor" />
        <Request Name="LockOpenDoor" />
        <Request Name="LockOpenReleaseDoor" />
        <Request Name="DoubleLockDoor" />
      </Requests>
    </Service>
    <Service SpecificationName="Imaging">
      <Requests>
        <Request Name="SetImagingSettings" />
        <Request Name="SetCurrentPreset" />
        <Request Name="Move" />
        <Request Name="Stop" />
      </Requests>
    </Service>
    <Service SpecificationName="Media">
      <Requests>
        <Request Name="CreateProfile" />
        <Request Name="AddVideoSourceConfiguration" />
        <Request Name="AddVideoEncoderConfiguration" />
        <Request Name="AddAudioSourceConfiguration" />
        <Request Name="AddAudioEncoderConfiguration" />
        <Request Name="AddPTZConfiguration" />
        <Request Name="AddVideoAnalyticsConfiguration" />
        <Request Name="AddMetadataConfiguration" />
        <Request Name="AddAudioOutputConfiguration" />
        <Request Name="AddAudioDecoderConfiguration" />
        <Request Name="RemoveVideoSourceConfiguration" />
        <Request Name="RemoveVideoEncoderConfiguration" />
        <Request Name="RemoveAudioSourceConfiguration" />
        <Request Name="RemoveAudioEncoderConfiguration" />
        <Request Name="RemovePTZConfiguration" />
        <Request Name="RemoveVideoAnalyticsConfiguration" />
        <Request Name="RemoveMetadataConfiguration" />
        <Request Name="RemoveAudioOutputConfiguration" />
        <Request Name="RemoveAudioDecoderConfiguration" />
        <Request Name="DeleteProfile" />
        <Request Name="SetVideoSourceConfiguration" />
```

```
        <Request Name="SetVideoEncoderConfiguration" />
        <Request Name="SetAudioSourceConfiguration" />
        <Request Name="SetAudioEncoderConfiguration" />
        <Request Name="SetVideoAnalyticsConfiguration" />
        <Request Name="SetMetadataConfiguration" />
        <Request Name="SetAudioOutputConfiguration" />
        <Request Name="SetAudioDecoderConfiguration" />
        <Request Name="StartMulticastStreaming" />
        <Request Name="StopMulticastStreaming" />
        <Request Name="SetSynchronizationPoint" />
        <Request Name="CreateOSD" />
        <Request Name="DeleteOSD" />
        <Request Name="SetOSD" />
      </Requests>
    </Service>
    <Service SpecificationName="Media2">
      <Requests>
        <Request Name="CreateProfile" />
        <Request Name="AddConfiguration" />
        <Request Name="RemoveConfiguration" />
        <Request Name="DeleteProfile" />
        <Request Name="CreateMultitrackConfiguration" />
        <Request Name="SetVideoSourceConfiguration" />
        <Request Name="SetAudioSourceConfiguration" />
        <Request Name="SetVideoEncoderConfiguration" />
        <Request Name="SetAudioEncoderConfiguration" />
        <Request Name="SetMetadataConfiguration" />
        <Request Name="SetAudioOutputConfiguration" />
        <Request Name="SetAudioDecoderConfiguration" />
        <Request Name="StartMulticastStreaming" />
        <Request Name="StopMulticastStreaming" />
        <Request Name="SetSynchronizationPoint" />
        <Request Name="CreateOSD" />
        <Request Name="DeleteOSD" />
        <Request Name="SetOSD" />
        <Request Name="CreateMask" />
        <Request Name="DeleteMask" />
        <Request Name="SetMask" />
      </Requests>
    </Service>
```

```
        <Service SpecificationName="PTZ">
          <Requests>
            <Request Name="SetConfiguration" />
            <Request Name="AbsoluteMove" />
            <Request Name="RelativeMove" />
            <Request Name="ContinuousMove" />
            <Request Name="GeoMove" />
            <Request Name="Stop" />
            <Request Name="MoveAndStartTracking" />
            <Request Name="SetPreset" />
            <Request Name="GotoPreset" />
            <Request Name="RemovePreset" />
            <Request Name="GotoHomePosition" />
            <Request Name="SetHomePosition" />
            <Request Name="SendAuxiliaryCommand" />
            <Request Name="CreatePresetTour" />
            <Request Name="ModifyPresetTour" />
            <Request Name="OperatePresetTour" />
            <Request Name="RemovePresetTour" />
          </Requests>
        </Service>
        <Service SpecificationName="Receiver">
          <Requests>
            <Request Name="CreateReceiver" />
            <Request Name="DeleteReceiver" />
            <Request Name="ConfigureReceiver" />
            <Request Name="SetReceiverMode" />
          </Requests>
        </Service>
        <Service SpecificationName="RecordingControl">
          <Requests>
            <Request Name="CreateRecording" />
            <Request Name="DeleteRecording" />
            <Request Name="SetRecordingConfiguration" />
            <Request Name="CreateTrack" />
            <Request Name="DeleteTrack" />
            <Request Name="SetTrackConfiguration" />
            <Request Name="CreateRecordingJob" />
            <Request Name="DeleteRecordingJob" />
            <Request Name="SetRecordingJobConfiguration" />
```

```
          <Request Name="SetRecordingJobMode" />
        </Requests>
      </Service>
      <Service SpecificationName="ReplayControl">
        <Requests>
          <Request Name="SetReplayConfiguration" />
        </Requests>
      </Service>
      <Service SpecificationName="Schedule">
        <Requests>
          <Request Name="GetScheduleState" />
        </Requests>
      </Service>
      <Service SpecificationName="Thermal">
        <Requests>
          <Request Name="SetConfiguration" />
          <Request Name="GetRadiometryConfiguration" />
          <Request Name="SetRadiometryConfiguration" />
        </Requests>
      </Service>
    </Services>
  </AccessGroup>
  <AccessGroup UserLevel="User">
    <Services>
      <Service SpecificationName="AccessControl">
        <Requests>
          <Request Name="GetAccessPointInfo" />
          <Request Name="GetAccessPointInfoList" />
          <Request Name="GetAccessPoints" />
          <Request Name="GetAccessPointList" />
          <Request Name="GetAreaInfo" />
          <Request Name="GetAreaInfoList" />
          <Request Name="GetAreas" />
          <Request Name="GetAreaList" />
        </Requests>
      </Service>
      <Service SpecificationName="AccessRules">
        <Requests>
          <Request Name="GetAccessProfileInfo" />
          <Request Name="GetAccessProfileInfoList" />
```

```
        <Request Name="GetAccessProfiles" />
        <Request Name="GetAccessProfileList" />
      </Requests>
    </Service>
    <Service SpecificationName="ActionEngine">
      <Requests>
        <Request Name="GetSupportedActions" />
        <Request Name="GetActions" />
        <Request Name="GetActionTriggers" />
      </Requests>
    </Service>
    <Service SpecificationName="AnalyticsEngine">
      <Requests>
        <Request Name="GetSupportedRules" />
        <Request Name="GetRules" />
        <Request Name="GetRuleOptions" />
        <Request Name="GetSupportedAnalyticsModules" />
        <Request Name="GetAnalyticsModules" />
        <Request Name="GetAnalyticsModuleOptions" />
        <Request Name="GetSupportedMetadata" />
      </Requests>
    </Service>
    <Service SpecificationName="AuthenticationBehavior">
      <Requests>
        <Request Name="GetAuthenticationProfileInfo" />
        <Request Name="GetAuthenticationProfileInfoList" />
        <Request Name="GetAuthenticationProfiles" />
        <Request Name="GetAuthenticationProfileList" />
        <Request Name="GetSecurityLevelInfo" />
        <Request Name="GetSecurityLevelInfoList" />
        <Request Name="GetSecurityLevels" />
        <Request Name="GetSecurityLevelList" />
      </Requests>
    </Service>
    <Service SpecificationName="Core">
      <Requests>
        <Request Name="GetDNS" />
        <Request Name="GetNTP" />
        <Request Name="GetDynamicDNS" />
        <Request Name="GetNetworkInterfaces" />
```

```
            <Request Name="GetNetworkProtocols" />
            <Request Name="GetNetworkDefaultGateway" />
            <Request Name="GetZeroConfiguration" />
            <Request Name="GetIPAddressFilter" />
            <Request Name="GetDot11Capabilities" />
            <Request Name="GetDot11Status" />
            <Request Name="ScanAvailableDot11Networks" />
            <Request Name="GetDeviceInformation" />
            <Request Name="GetSystemUris" />
            <Request Name="GetScopes" />
            <Request Name="GetDiscoveryMode" />
            <Request Name="GetGeoLocation" />
            <Request Name="GetRemoteUser" />
            <Request Name="GetPasswordComplexityOptions" />
            <Request Name="GetPasswordComplexityConfiguration" />
            <Request Name="GetPasswordHistoryConfiguration" />
            <Request Name="GetAuthFailureWarningOptions" />
            <Request Name="GetAuthFailureWarningConfiguration" />
            <Request Name="GetRelayOutputs" />
            <Request Name="GetStorageConfigurations" />
            <Request Name="GetStorageConfiguration" />
            <Request Name="CreatePullPointSubscription" />
            <Request Name="PullMessages" />
            <Request Name="Renew" />
            <Request Name="Unsubscribe" />
            <Request Name="Seek" />
            <Request Name="SetSynchronizationPoint" />
            <Request Name="GetEventProperties" />
            <Request Name="GetEventBrokers" />
          </Requests>
        </Service>
        <Service SpecificationName="Credential">
          <Requests>
            <Request Name="GetCredentialInfo" />
            <Request Name="GetSupportedFormatTypes" />
            <Request Name="GetCredentialAccessProfiles" />
          </Requests>
        </Service>
        <Service SpecificationName="DeviceIO">
          <Requests>
```

```
        <Request Name="GetVideoOutputs" />
        <Request Name="GetVideoOutputConfiguration" />
        <Request Name="GetVideoSources" />
        <Request Name="GetAudioOutputs" />
        <Request Name="GetAudioSources" />
        <Request Name="GetRelayOutputs" />
        <Request Name="GetDigitalInputs" />
        <Request Name="GetDigitalInputConfigurationOptions" />
        <Request Name="GetSerialPorts" />
        <Request Name="GetSerialPortConfiguration" />
        <Request Name="GetSerialPortConfigurationOptions" />
      </Requests>
    </Service>
    <Service SpecificationName="Display">
      <Requests>
        <Request Name="GetPaneConfigurations" />
        <Request Name="GetPaneConfiguration" />
        <Request Name="GetLayout" />
        <Request Name="GetDisplayOptions" />
      </Requests>
    </Service>
    <Service SpecificationName="DoorControl">
      <Requests>
        <Request Name="GetDoorInfo" />
        <Request Name="GetDoorInfoList" />
        <Request Name="GetDoors" />
        <Request Name="GetDoorList" />
        <Request Name="GetDoorState" />
      </Requests>
    </Service>
    <Service SpecificationName="Imaging">
      <Requests>
        <Request Name="GetPresets" />
        <Request Name="GetCurrentPreset" />
        <Request Name="GetMoveOptions" />
        <Request Name="GetStatus" />
      </Requests>
    </Service>
    <Service SpecificationName="Media">
      <Requests>
```

```
            <Request Name="GetProfiles" />
            <Request Name="GetProfile" />
            <Request Name="GetVideoSources" />
            <Request Name="GetVideoSourceConfigurations" />
            <Request Name="GetVideoSourceConfiguration" />
            <Request Name="GetCompatibleVideoSourceConfigurations" />
            <Request Name="GetVideoSourceConfigurationOptions" />
            <Request Name="GetVideoEncoderConfigurations" />
            <Request Name="GetVideoEncoderConfiguration" />
            <Request Name="GetCompatibleVideoEncoderConfigurations" />
            <Request Name="GetVideoEncoderConfigurationOptions" />
            <Request Name="GetGuaranteedNumberOfVideoEncoderInstances" />
            <Request Name="GetAudioSources" />
            <Request Name="GetAudioSourceConfigurations" />
            <Request Name="GetAudioSourceConfiguration" />
            <Request Name="GetCompatibleAudioSourceConfigurations" />
            <Request Name="GetAudioSourceConfigurationOptions" />
            <Request Name="GetAudioEncoderConfigurations" />
            <Request Name="GetAudioEncoderConfiguration" />
            <Request Name="GetCompatibleAudioEncoderConfigurations" />
            <Request Name="GetAudioEncoderConfigurationOptions" />
            <Request Name="GetVideoAnalyticsConfigurations" />
            <Request Name="GetVideoAnalyticsConfiguration" />
            <Request Name="GetCompatibleVideoAnalyticsConfigurations" />
            <Request Name="GetMetadataConfigurations" />
            <Request Name="GetMetadataConfiguration" />
            <Request Name="GetCompatibleMetadataConfigurations" />
            <Request Name="GetMetadataConfigurationOptions" />
            <Request Name="GetAudioOutputs" />
            <Request Name="GetAudioOutputConfigurations" />
            <Request Name="GetAudioOutputConfiguration" />
            <Request Name="GetCompatibleAudioOutputConfigurations" />
            <Request Name="GetAudioOutputConfigurationOptions" />
            <Request Name="GetAudioDecoderConfigurations" />
            <Request Name="GetAudioDecoderConfiguration" />
            <Request Name="GetCompatibleAudioDecoderConfigurations" />
            <Request Name="GetAudioDecoderConfigurationOptions" />
            <Request Name="GetStreamUri" />
            <Request Name="GetSnapshotUri" />
            <Request Name="GetVideoSourceModes" />
```

```
      <Request Name="GetOSDs" />
      <Request Name="GetOSD" />
      <Request Name="GetOSDOptions" />
    </Requests>
  </Service>
  <Service SpecificationName="Media2">
    <Requests>
      <Request Name="GetProfiles" />
      <Request Name="GetVideoSourceConfigurations" />
      <Request Name="GetAudioSourceConfigurations" />
      <Request Name="GetVideoEncoderConfigurations" />
      <Request Name="GetAudioEncoderConfigurations" />
      <Request Name="GetMetadataConfigurations" />
      <Request Name="GetAudioOutputConfigurations" />
      <Request Name="GetAudioDecoderConfigurations" />
      <Request Name="GetAnalyticsConfigurations" />
      <Request Name="GetVideoSourceConfigurationOptions" />
      <Request Name="GetAudioSourceConfigurationOptions" />
      <Request Name="GetVideoEncoderConfigurationOptions" />
      <Request Name="GetAudioEncoderConfigurationOptions" />
      <Request Name="GetMetadataConfigurationOptions" />
      <Request Name="GetAudioOutputConfigurationOptions" />
      <Request Name="GetAudioDecoderConfigurationOptions" />
      <Request Name="GetVideoEncoderInstances" />
      <Request Name="GetStreamUri" />
      <Request Name="GetSnapshotUri" />
      <Request Name="GetVideoSourceModes" />
      <Request Name="GetOSDs" />
      <Request Name="GetOSDOptions" />
      <Request Name="GetMasks" />
      <Request Name="GetMaskOptions" />
    </Requests>
  </Service>
  <Service SpecificationName="Provisioning">
    <Requests>
      <Request Name="GetUsage" />
    </Requests>
  </Service>
  <Service SpecificationName="PTZ">
    <Requests>
```

```
        <Request Name="GetNodes" />
        <Request Name="GetNode" />
        <Request Name="GetConfigurations" />
        <Request Name="GetConfiguration" />
        <Request Name="GetConfigurationOptions" />
        <Request Name="GetCompatibleConfigurations" />
        <Request Name="GetStatus" />
        <Request Name="GetPresets" />
        <Request Name="GetPresetTours" />
        <Request Name="GetPresetTour" />
        <Request Name="GetPresetTourOptions" />
      </Requests>
    </Service>
    <Service SpecificationName="RecordingControl">
      <Requests>
        <Request Name="GetRecordings" />
        <Request Name="GetRecordingConfiguration" />
        <Request Name="GetTrackConfiguration" />
        <Request Name="GetRecordingJobs" />
        <Request Name="GetRecordingJobConfiguration" />
        <Request Name="GetRecordingJobState" />
        <Request Name="GetRecordingOptions" />
        <Request Name="ExportRecordedData" />
        <Request Name="StopExportRecordedData" />
        <Request Name="GetExportRecordedDataState" />
      </Requests>
    </Service>
    <Service SpecificationName="RecordingSearch">
      <Requests>
        <Request Name="GetRecordingSummary" />
        <Request Name="GetRecordingInformation" />
        <Request Name="GetMediaAttributes" />
        <Request Name="FindRecordings" />
        <Request Name="GetRecordingSearchResults" />
        <Request Name="FindEvents" />
        <Request Name="GetEventSearchResults" />
        <Request Name="FindPTZPosition" />
        <Request Name="GetPTZPositionSearchResults" />
        <Request Name="FindMetadata" />
        <Request Name="GetMetadataSearchResults" />
```

```
        </Requests>
      </Service>
      <Service SpecificationName="ReplayControl">
        <Requests>
          <Request Name="GetReplayUri" />
          <Request Name="GetReplayConfiguration" />
        </Requests>
      </Service>
      <Service SpecificationName="Schedule">
        <Requests>
          <Request Name="GetScheduleInfo" />
          <Request Name="GetScheduleInfoList" />
          <Request Name="GetSchedules" />
          <Request Name="GetScheduleList" />
          <Request Name="GetSpecialDayGroupInfo" />
          <Request Name="GetSpecialDayGroupInfoList" />
          <Request Name="GetSpecialDayGroups" />
          <Request Name="GetSpecialDayGroupList" />
        </Requests>
      </Service>
      <Service SpecificationName="Security">
        <Requests>
          <Request Name="CreatePKCS10CSR" />
          <Request Name="GetClientAuthenticationRequired" />
          <Request Name="GetCnMapsToUser" />
          <Request Name="GetEnabledTLSVersions" />
        </Requests>
      </Service>
      <Service SpecificationName="Thermal">
        <Requests>
          <Request Name="GetConfiguration" />
          <Request Name="GetConfigurationOptions" />
          <Request Name="GetConfigurations" />
          <Request Name="GetRadiometryConfigurationOptions" />
        </Requests>
      </Service>
    </Services>
  </AccessGroup>
  <AccessGroup UserLevel="Anonymous">
    <Services>
```

```
<Service SpecificationName="AccessControl">
  <Requests>
    <Request Name="GetServiceCapabilities" />
  </Requests>
</Service>
<Service SpecificationName="AccessRules">
  <Requests>
    <Request Name="GetServiceCapabilities" />
  </Requests>
</Service>
<Service SpecificationName="ActionEngine">
  <Requests>
    <Request Name="GetServiceCapabilities" />
  </Requests>
</Service>
<Service SpecificationName="AnalyticsEngine">
  <Requests>
    <Request Name="GetServiceCapabilities" />
  </Requests>
</Service>
<Service SpecificationName="ApplicationManagement">
  <Requests>
    <Request Name="GetCapabilities" />
  </Requests>
</Service>
<Service SpecificationName="AuthenticationBehavior">
  <Requests>
    <Request Name="GetServiceCapabilities" />
  </Requests>
</Service>
<Service SpecificationName="Core">
  <Requests>
    <Request Name="GetWsdlUrl" />
    <Request Name="GetServices" />
    <Request Name="GetServiceCapabilities" />
    <Request Name="GetCapabilities" />
    <Request Name="GetHostname" />
    <Request Name="GetSystemDateAndTime" />
    <Request Name="GetEndpointReference" />
  </Requests>
```

```
    </Service>
    <Service SpecificationName="Credential">
      <Requests>
        <Request Name="GetServiceCapabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="DeviceIO">
      <Requests>
        <Request Name="GetRelayOutputOptions" />
        <Request Name="GetServiceCapabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="Display">
      <Requests>
        <Request Name="Capabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="DoorControl">
      <Requests>
        <Request Name="GetServiceCapabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="Imaging">
      <Requests>
        <Request Name="GetServiceCapabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="Media">
      <Requests>
        <Request Name="GetServiceCapabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="Media2">
      <Requests>
        <Request Name="GetServiceCapabilities" />
      </Requests>
    </Service>
    <Service SpecificationName="Provisioning">
      <Requests>
        <Request Name="GetServiceCapabilities" />
```

```
    </Requests>
  </Service>
  <Service SpecificationName="PTZ">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="Receiver">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="RecordingControl">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="RecordingSearch">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="ReplayControl">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="Schedule">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="Security">
    <Requests>
      <Request Name="GetServiceCapabilities" />
    </Requests>
  </Service>
  <Service SpecificationName="Thermal">
    <Requests>
      <Request Name="GetServiceCapabilities" />
```

```
          </Requests>
        </Service>
      </Services>
    </AccessGroup>
  </AccessGroups>
</AccessPolicyDefinition>
```

A.3 Create user with defined user level

Name: HelperCreateUserLevel

Procedure Purpose: Helper procedure to create user with predefined user level or change existing with new one.

Pre-requisite: GetServices command is supported by the DUT. Maximum Username Length is supported by the DUT as indicated by the Capabilities.Security.MaxUsernameLength, Maximum Password Length is supported by the DUT as indicated by the Capabilities.Security.MaxPasswordLength.

Input: The user level (*userLevel*) of user to be created (*userLevel* shall have User or Operator value).

Returns: The user login (*userLogin*) with predefined user level and corresponding user password (*password*).

Procedure:

1. ONVIF Client gets the service capabilities (out *cap*) by following the procedure mentioned in Annex A.4.
2. If *cap* does not contain Security.MaxPasswordLength or Security.MaxUserNameLength, FAIL the test and skip other steps.
3. ONVIF Client invokes **GetUsers**.
4. The DUT responds with a **GetUsersResponse** message with parameters
   - User list := userList
5. If there is user with user level userLevel in userList:

   5.1. Set the following:

   - *passwordLength* := cap.Security.MaxPasswordLength

- *userLogin* := Username of user with user level equal to userLevel from *userList*
- *password* := random string, contains passwordLength ASCII characters

5.2. ONVIF Client invokes **SetUser** with parameters

- User[0].Username := *userLogin*
- User[0].Password := *password*
- User[0].UserLevel := *userLevel*
- Extension skipped

5.3. If the DUT responds with **SetUserResponse** message, skip other steps.

5.4. If the DUT returns env:Sender\ter:OperationProhibited\ter:Password SOAP 1.2 fault:

5.4.1. Set the following:

- *password* := random string, contains *password*Length ASCII characters

5.4.2. Go to the step 6.2.

5.5. If DUT returns other SOAP 1.2 fault, FAIL the test and skip other steps.

6. If there are no users with user level *userLevel* in *userList*:

6.1. Set the following:

- *userLoginLength* := *cap*.Security.MaxUserNameLength
- *passwordLength* := *cap*.Security.MaxPasswordLength
- *userLogin* := random string, contains *userLoginLength* low case alphbet characters, differs from usernames listed in *userList*
- *password* := random string, contains *passwordLength* ASCII characters

6.2. ONVIF Client invokes **CreateUsers** with parameters

- User[0].Username := *userLogin*
- User[0].Password := *password*
- User[0].UserLevel := *userLevel*
- Extension skipped

6.3. If the DUT responds with **CreateUsersResponse** message, skip other steps.

6.4. If the DUT returns env:Sender\ter:OperationProhibited\ter:Password SOAP 1.2 fault:

6.4.1. Set the following:

- *password* := random string, contains *passwordLength* ASCII characters

6.4.2. Go to the step 7.2.

6.4.3. If the DUT returns other SOAP 1.2 fault, FAIL the test and skip other steps.

Procedure Result:

PASS –

- The DUT passed all assertions.

FAIL –

- The DUT did not send **GetServiceCapabilitiesResponse** message.
- The DUT did not send **GetUsersResponse** message.

Note: ONVIF client uses password values from Management tab for CreateUsers and StUser operations if 'Provide own passwords' is active on Management tab.

A.4 Get service capabilities

Name: HelperGetServiceCapabilities

Procedure Purpose: Helper procedure to get device service capabilities.

Pre-requisite: None.

Input: None.

Returns: The service capabilities (*cap*).

Procedure:

1. ONVIF Client invokes **GetServiceCapabilities**.
2. The DUT responds with a **GetServiceCapabilitiesResponse** message with parameters
   - Capabilities =: *cap*

Procedure Result:

PASS –

- The DUT passed all assertions.

FAIL –

- The DUT did not send **GetServiceCapabilitiesResponse** message.

A.5 Acceptable Faults

On the Management tab test operator can choose which faults are treated as PASSED in the ACCESS_POLICY-1-1-1 ACCESS POLICY (ACCESS NOT ALLOWED) test case:

- ter:ActionNotSupported
- ter:ActionNotSupported/subcode