

ONVIF®

Add-Ons Conformance Device Test Specification

Version 26.06

February 2026

© 2026 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
23.06	Nov, 16	First issue
24.12	Nov, 15	The following test and annexes were updated according #209: Steps 3.7 and 3.8 were added at ONVIF TLS Configuration Add-on Support Check section
26.06	Feb, 09	The following test and annexes were updated according #462: TLS Configuration 2.0 Add-On Conformance Editorial changes were done
26.06	Apr, 07	The following test and annexes were updated according #372: Profile V Security 1.0 Add-On Conformance
26.06	Apr, 10	The following test and annexes were updated according #526: Media signing 1.0 Add-On Conformance
26.06	May 11, 2026	The following were added/updated for ONVIF Media Signing 1.0 Add-on according #618: GetVideoEncoderConfigurationOptions (Media2) was added under Media profile configuration for Signed Video feature group H.264 and H.265 support check was changed

Table of Contents

1	Introduction	5
1.1	Scope	5
1.2	Normative references	5
1.3	Informative References	6
1.4	Requirement by the Add-on	6
2	Terms and Definitions	7
2.1	Definitions	7
2.2	Abbreviations	7
3	ONVIF TLS Configuration 1.0 Add-On Conformance	8
3.1	Feature category classification for ONVIF TLS Configuration 1.0 Add-on Conformance	8
3.2	ONVIF TLS Configuration 1.0 Add-on Support Check	9
4	ONVIF TLS Configuration 2.0 Add-On Conformance	13
4.1	Feature category classification for ONVIF TLS Configuration 2.0 Add-on Conformance	13
4.2	ONVIF TLS Configuration 2.0 Add-on Support Check	14
5	ONVIF Media Signing 1.0 Add-On Conformance	19
5.1	Feature category classification for ONVIF Media Signing 1.0 Add-on Conformance	19
5.2	ONVIF Media Signing 1.0 Add-on Support Check	20
6	ONVIF Profile V Security 1.0 Add-On Conformance	23
6.1	Feature category classification for ONVIF Profile V Security 1.0 Add-On Conformance	23
6.2	ONVIF Profile V Security 1.0 Add-on Support Check	25

1 Introduction

The goal of the ONVIF Add-Ons Conformance Test Specification document is to provide some details about logic of add-on's supporting check.

ONVIF TLS Configuration 1.0 Add-On Conformance item focuses on ONVIF TLS Configuration Add-on Specification ([ONVIF TLS 1.0 Add-on]) as a referenced Add-on by an ONVIF device implementation under test.

ONVIF TLS Configuration 2.0 Add-On Conformance item focuses on ONVIF TLS Configuration Add-on Specification ([ONVIF TLS 2.0 Add-on]) as a referenced Add-on by an ONVIF device implementation under test.

ONVIF Media Signing 1.0 Add-On Conformance item focuses on ONVIF Media Signing Add-on Specification ([ONVIF Media Signing 1.0 Add-on]) as a referenced Add-on by an ONVIF device implementation under test.

ONVIF Profile V Security 1.0 Add-On Conformance item focuses on ONVIF Profile-V Security Add-on Specification ([ONVIF Profile V Security 1.0 Add-on]) as a referenced Add-on by an ONVIF device implementation under test.

1.1 Scope

This ONVIF Add-Ons Conformance Test Specification document defines and regulates the conformance testing procedure for the ONVIF conformant devices. The objective of this specification is to provide the logic of ONVIF Add-Ons detection according to [ONVIF TLS 1.0 Add-on], [ONVIF TLS 2.0 Add-on], [ONVIF Profile V Security 1.0 Add-on], [ONVIF Media Signing 1.0 Add-on].

1.2 Normative references

- [ONVIF Network Interface Specs] ONVIF Network Interface Specification documents:
<https://www.onvif.org/profiles/specifications/>
- [ONVIF Conformance] ONVIF Conformance Process Specification:
<https://www.onvif.org/profiles/conformance/>
- [ONVIF TLS 1.0 Add-on] ONVIF TLS Configuration 1.0 Add-on Specification:
<https://www.onvif.org/profiles/add-on/>
- [ONVIF TLS 2.0 Add-on] ONVIF TLS Configuration 2.0 Add-on Specification:

<https://www.onvif.org/profiles/add-on/>

- [ONVIF Media Signing 1.0 Add-on] ONVIF Media Signing Add-on Specification:

<https://www.onvif.org/profiles/add-on/>

- [ONVIF Profile V Security 1.0 Add-on] ONVIF Profile-V Security Add-on Specification:

<https://www.onvif.org/profiles/add-on/>

1.3 Informative References

- [ONVIF Feature Discovery] ONVIF Feature Discovery Specification:

<https://www.onvif.org/profiles/conformance/device-test-2/>

1.4 Requirement by the Add-on

The following define denotations to indicate the required level by the Add-on towards ONVIF device implementation (DUT).

M = mandatory function that shall be SUPPORTED by DUT

C = conditional mandatory function that shall be SUPPORTED by DUT if they support that functionality. On the list of test cases such functionalities are described after C - the content of parenthesis.

2 Terms and Definitions

2.1 Definitions

Add-on See ONVIF Profile Policy.

2.2 Abbreviations

This section describes abbreviations used in this document.

DUT Device Under Test

3 ONVIF TLS Configuration 1.0 Add-On Conformance

3.1 Feature category classification for ONVIF TLS Configuration 1.0 Add-on Conformance

In order for ONVIF Device Test Tool to conduct conformance testing toward [ONVIF TLS 1.0 Add-on], it would need to identify whether DUT implements the expected feature set.

This section classifies supported features as multiple categories that are related to [ONVIF TLS 1.0 Add-on] conformance. Those category classifications will be used to do some preliminary checking prior to the test case execution and also they will be used to determine whether DUT can be considered to be [ONVIF TLS 1.0 Add-on] conformant device.

The following discovery scope is defined as the scope that signals that DUT is [ONVIF TLS 1.0 Add-on] product.

Table 3.1. TLS Configuration 1.0 Add-On Capability

TLSServerConfiguration

The following table shows the classified feature categories based on commands and/or functional blocks that are referenced by DUT.

Table 3.2. ONVIF TLS Configuration 1.0 Add-on Conformance Features Categories

Add-on Mandatory Features	
Discovery	GetServiceCapabilities (Device Management)
TLS Server Configuration	AddServerCertificateAssignment (Security Configuration)
	CreateCertificationPath (Security Configuration)
	CreatePKCS10CSR (Security Configuration)
	CreateRSAKeyPair (Security Configuration)
	CreateSelfSignedCertificate (Security Configuration)
	DeleteCertificate (Security Configuration)
	DeleteCertificationPath (Security Configuration)
	DeleteKey (Security Configuration)

GetAllCertificates (Security Configuration)
GetAllCertificationPaths (Security Configuration)
GetAllKeys (Security Configuration)
GetAssignedServerCertificates (Security Configuration)
GetCertificate (Security Configuration)
GetCertificationPath (Security Configuration)
GetKeyStatus (Security Configuration)
tns1:Advancedsecurity/Keystore/KeyStatus (Event)
RemoveServerCertificateAssignment (Security Configuration)
ReplaceServerCertificateAssignment (Security Configuration)
SetNetworkProtocols (Device Management)
ReplaceServerCertificateAssignment (Security Configuration)

3.2 ONVIF TLS Configuration 1.0 Add-on Support Check

Preliminary checking for feature discovery will be performed prior to the test execution. For the details of the preliminary feature discovery, refer to [ONVIF Feature Discovery].

According to the result of test case execution, final determination of [ONVIF TLS 1.0 Add-on] support toward DUT is performed based on the following procedure.

Procedure:

1. Check that Addons list contains the text given in [Table 3.1](#). If there is no such text at Addons list of the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported and other steps will be skipped.
2. Check Device Management Service related features:
 - 2.1. Check that GetServices command is supported by the DUT. If **Device Service/Capabilities/GetServices** is not supported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by DUT and certification will be failed. Otherwise, then it is determined that the following features are supported by the DUT:
 - i. Discovery feature category:

- GetServiceCapabilities (Device Management)
- 2.2. The following features are supported by the DUT, because these are mandatory features for any ONVIF device implementation:
- i. TLS Server Configuration feature category:
 - SetNetworkProtocols (Device Management)
3. Check that Security Configuration Service is supported by the DUT. If **Security Configuration Service** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by the DUT and certification will be failed. Otherwise:
- 3.1. Check that RSA Key Pair Generation is supported by the DUT. If **Security Configuration Service\Keystore features support\RSA Key Pair Generation** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by the DUT and certification will be failed. Otherwise, then it is determined that the following features are supported by the DUT:
- i. TLS Server Configuration feature category:
 - CreateRSAKeyPair (Security Configuration)
 - GetKeyStatus (Security Configuration)
 - GetAllKeys (Security Configuration)
 - DeleteKey (Security Configuration)
 - tns1:Advancedsecurity/Keystore/KeyStatus (Event)
- 3.2. If DUT does not returns MaximumNumberOfKeys or returns MaximumNumberOfKeys less than 16, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by DUT and certification will be failed.
- 3.3. Check that Self-Signed Certificate Creation with RSA is supported by the DUT. If **Security Configuration Service\Keystore features support\Self-Signed Certificate Creation with RSA** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by the DUT and certification will be failed. Otherwise, then it is determined that the following features are supported by the DUT:
- i. TLS Server Configuration feature category:

- CreateSelfSignedCertificate (Security Configuration)
 - GetCertificate (Security Configuration)
 - GetAllCertificates (Security Configuration)
 - DeleteCertificate (Security Configuration)
- 3.4. Check that PKCS10 External Certification with RSA is supported by the DUT. If **Security Configuration Service\Keystore features support\PKCS10 External Certification with RSA** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by the DUT and certification will be failed. Otherwise, then it is determined that the following features are supported by the DUT:
- i. TLS Server Configuration feature category:
- CreatePKCS10CSR (Security Configuration)
 - GetCertificate (Security Configuration)
 - GetAllCertificates (Security Configuration)
 - DeleteCertificate (Security Configuration)
 - UploadCertificate (Security Configuration)
- 3.5. If DUT does not return MaximumNumberOfCertificates or returns MaximumNumberOfCertificates less than 16, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by DUT and certification will be failed.
- 3.6. Check that TLS Server Support is supported by the DUT. If **Security Configuration Service\TLS features support\TLS Server Support** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by the DUT and certification will be failed. Otherwise, then it is determined that the following features are supported by the DUT:
- i. TLS Server Configuration feature category:
- CreateCertificationPath (Security Configuration)
 - GetCertificationPath (Security Configuration)
 - GetAllCertificationPaths (Security Configuration)
 - DeleteCertificationPath (Security Configuration)

- AddServerCertificateAssignment (Security Configuration)
- RemoveServerCertificateAssignment (Security Configuration)
- ReplaceServerCertificateAssignment (Security Configuration)
- GetAssignedServerCertificates (Security Configuration)

3.7. If **Security Configuration Service\Keystore features support\Signature Algorithm \1.2.840.113549.1.1.5** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by DUT and certification will be failed.

3.8. If **Security Configuration Service\Keystore features support\Signature Algorithm \1.2.840.113549.1.1.11** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 1.0 Add-on] is not supported by DUT and certification will be failed.

4 ONVIF TLS Configuration 2.0 Add-On Conformance

4.1 Feature category classification for ONVIF TLS Configuration 2.0 Add-on Conformance

In order for ONVIF Device Test Tool to conduct conformance testing toward [ONVIF TLS 2.0 Add-on], it would need to identify whether DUT implements the expected feature set.

This section classifies supported features as multiple categories that are related to [ONVIF TLS 2.0 Add-on] conformance. Those category classifications will be used to do some preliminary checking prior to the test case execution and also they will be used to determine whether DUT can be considered to be [ONVIF TLS 2.0 Add-on] conformant device.

The following discovery scope is defined as the scope that signals that DUT is [ONVIF TLS 2.0 Add-on] product.

Table 4.1. TLS Configuration 2.0 Add-On Capability

TLSServerConfiguration_v2

The following table shows the classified feature categories based on commands and/or functional blocks that are referenced by DUT.

Table 4.2. ONVIF TLS Configuration 2.0 Add-on Conformance Features Categories

Add-on Mandatory Features	
Discovery	GetServices (Device Management)
	GetServiceCapabilities (Device Management)
TLS Configuration	AddServerCertificateAssignment (Security Configuration)
	CreateCertificationPath (Security Configuration)
	CreatePKCS10CSR (Security Configuration)
	CreateRSAKeyPair (Security Configuration)
	CreateECKKeyPair (Security Configuration)
	CreateSelfSignedCertificate (Security Configuration)

DeleteCertificate (Security Configuration)
DeleteCertificationPath (Security Configuration)
DeleteKey (Security Configuration)
GetAllCertificates (Security Configuration)
GetAllCertificationPaths (Security Configuration)
GetAllKeys (Security Configuration)
GetAssignedServerCertificates (Security Configuration)
GetCertificate (Security Configuration)
GetCertificationPath (Security Configuration)
GetKeyStatus (Security Configuration)
GetServiceCapabilities (Security Configuration)
tns1:Advancedsecurity/Keystore/KeyStatus (Event)
RemoveServerCertificateAssignment (Security Configuration)
ReplaceServerCertificateAssignment (Security Configuration)
SetNetworkProtocols (Device Management)
UploadCertificate (Security Configuration)

4.2 ONVIF TLS Configuration 2.0 Add-on Support Check

Preliminary checking for feature discovery will be performed prior to the test execution. For the details of the preliminary feature discovery, refer to [ONVIF Feature Discovery].

According to the result of feature discovery execution, final determination of [ONVIF TLS 2.0 Add-on] support toward DUT is performed based on the following procedure.

After this test cases required for the features determinate at feature discovery will be executed.

Procedure:

1. Check that Addons list capability contains item with equal to given in [Table 4.1](#).

If there is no such item at Addons list capability of the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported and other steps will be skipped.

2. Check Device Management Service related features:

2.1. Check that GetServices command is supported by the DUT.

If **Device Service/Capabilities/GetServices** feature is not supported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by DUT and certification will be failed.

Otherwise, it is determined that the following features are supported by the DUT:

- i. Discovery feature category:
 - GetServices (Device Management)
 - GetServiceCapabilities (Device Management)

2.2. Check that Network Configuration is supported by the DUT.

If **Device Service\System\Network Configuration** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - SetNetworkProtocols (Device Management)

3. Check that Security Configuration Service is supported by the DUT.

If **Security Configuration Service** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise the following will be done:

3.1. It is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - GetServiceCapabilities (Security Configuration)

3.2. Check that Key Pair Generation is supported by the DUT.

If **Security Configuration Service\Keystore features support\Key Pair Generation** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - GetKeyStatus (Security Configuration)
 - GetAllKeys (Security Configuration)
 - DeleteKey (Security Configuration)
 - tns1:Advancedsecurity/Keystore/KeyStatus (Event)

3.3. Check that RSA Key Pair Generation is supported by the DUT.

If **Security Configuration Service\Keystore features support\Key Pair Generation\RSA** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - CreateRSAKeyPair (Security Configuration)

3.4. Check that ECC Key Pair Generation is supported by the DUT.

If **Security Configuration Service\Keystore features support\Key Pair Generation\ECC** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - CreateECKKeyPair (Security Configuration)

3.5. If DUT does not returns MaximumNumberOfKeys or returns MaximumNumberOfKeys less than 16, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by DUT and certification will be failed.

3.6. Check that Self-Signed Certificate Creation is supported by the DUT.

If **Security Configuration Service\Keystore features support\Self-Signed Certificate Creation** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - CreateSelfSignedCertificate (Security Configuration)
 - GetCertificate (Security Configuration)
 - GetAllCertificates (Security Configuration)
 - DeleteCertificate (Security Configuration)

3.7. Check that PKCS10 External Certification is supported by the DUT.

If **Security Configuration Service\Keystore features support\PKCS10 External Certification** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Configuration feature category:
 - CreatePKCS10CSR (Security Configuration)
 - GetCertificate (Security Configuration)
 - GetAllCertificates (Security Configuration)
 - DeleteCertificate (Security Configuration)
 - UploadCertificate (Security Configuration)

3.8. If DUT does not return MaximumNumberOfCertificates or returns MaximumNumberOfCertificates less than 16, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by DUT and certification will be failed.

3.9. Check that TLS Server Support is supported by the DUT.

If **Security Configuration Service\TLS features support\TLS Server Support** is regarded as unsupported by the DUT, then it is determined that [ONVIF TLS 2.0 Add-on] is not supported by the DUT and certification will be failed.

Otherwise, then it is determined that the following features are supported by the DUT:

- i. TLS Server Configuration feature category:
 - CreateCertificationPath (Security Configuration)

- GetCertificationPath (Security Configuration)
- GetAllCertificationPaths (Security Configuration)
- DeleteCertificationPath (Security Configuration)
- AddServerCertificateAssignment (Security Configuration)
- RemoveServerCertificateAssignment (Security Configuration)
- ReplaceServerCertificateAssignment (Security Configuration)
- GetAssignedServerCertificates (Security Configuration)

5 ONVIF Media Signing 1.0 Add-On Conformance

5.1 Feature category classification for ONVIF Media Signing 1.0 Add-on Conformance

In order for ONVIF Device Test Tool to conduct conformance testing toward [ONVIF Media Signing 1.0 Add-on], it would need to identify whether DUT implements the expected feature set.

This section classifies supported features as multiple categories that are related to [ONVIF Media Signing 1.0 Add-on] conformance. Those category classifications will be used to do some preliminary checking prior to the test case execution and also they will be used to determine whether DUT can be considered to be [ONVIF Media Signing 1.0 Add-on] conformant device.

The following discovery scope is defined as the scope that signals that DUT is [ONVIF Media Signing 1.0 Add-on] product.

Table 5.1. Media Signing 1.0 Add-On Capability

MediaSigning_v1

The following table shows the classified feature categories based on commands and/or functional blocks that are referenced by DUT.

Table 5.2. ONVIF Media Signing 1.0 Add-on Conformance Features Categories

Add-on Mandatory Features	
Discovery	GetServices (Device Management)
	GetServiceCapabilities (Device Management)
	GetServiceCapabilities (Media2)
	GetServiceCapabilities (Security Configuration)
Media profile configuration for Signed Video	GetServiceCapabilities (Media2)
	GetProfiles (Media2)
	GetVideoEncoderConfigurations (Media2)
	GetVideoEncoderConfigurationOptions (Media2)
	SetVideoEncoderConfiguration (Media2)
	SetSynchronizationPoint (Media2)
	GetStreamUri (Media2)

Security configuration for Signed Video	Video streaming using RTSP (Media2)
	Video Streaming over RTP/UDP-Unicast (Media2)
	Video Streaming over RTP/RTSP/HTTP/TCP (Media2)
	GetAssignedMediaSigningCertificates (Security Configuration)
	GetCertificationPath (Security Configuration)
	GetCertificate (Security Configuration)
	GetAssignedMediaSigningCertificates (Streaming)

5.2 ONVIF Media Signing 1.0 Add-on Support Check

Preliminary checking for feature discovery will be performed prior to the test execution. For the details of the preliminary feature discovery, refer to [ONVIF Feature Discovery].

According to the result of feature discovery execution, final determination of [ONVIF Media Signing 1.0 Add-on] support toward DUT is performed based on the following procedure.

After this test cases required for the features determinate at feature discovery will be executed.

Procedure:

1. Check that Addons list capability contains item with equal to given in [Table 5.1](#).

If there is no such item at Addons list capability of the DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported and other steps will be skipped.

2. Check Device Management Service related features:

- 2.1. Check that GetServices command is supported by the DUT.

If **Device Service/Capabilities/GetServices** feature is not supported by the DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by DUT and certification will be failed.

Otherwise, it is determined that the following features are supported by the DUT:

- i. Discovery feature category:
 - GetServices (Device Management)
 - GetServiceCapabilities (Device Management)

3. Check that Media2 Service is supported by the DUT. If **Media2 Service** is regarded as unsupported by the DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:
 - 3.1. It is determined that the following features are supported by the DUT:
 - i. Discovery feature category:
 - GetServiceCapabilities (Media2)
 - ii. Media profile configuration for Signed Video feature category:
 - GetServiceCapabilities (Media2)
 - GetProfiles (Media2)
 - 3.2. Check that Video Encoder Configuration is supported by the DUT. If **Media2 Service/Video Encoder Configuration** is regarded as unsupported by DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:
 - 3.2.1. It is determined that the following features are supported by the DUT:
 - i. Media profile configuration for Signed Video feature category:
 - GetVideoEncoderConfigurations (Media2)
 - SetVideoEncoderConfiguration (Media2)
 - GetVideoEncoderConfigurationOptions (Media2)
 - 3.2.2. Check that Signing supported by the DUT H.264 or H.265 encoding. If both **Media2 Service/Media Signing/H.264** and **Media2 Service/Media Signing/H.265** is regarded as unsupported by DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be FAILED.
 - 3.3. Check that Media Signing is supported by the DUT. If **Media2 Service/Media Signing** is regarded as unsupported by DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be FAILED.
 - 3.4. Check that RTSP streaming is supported by the DUT. If **Media2 Service/Real-time Streaming** is regarded as unsupported by DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be failed. Otherwise:

3.4.1. It is determined that the following features are supported by the DUT:

i. Media profile configuration for Signed Video feature category:

- GetStreamUri (Media2)
- Video Streaming using RTSP (Media2)
- Video Streaming over RTP/UDP-Unicast (Media2)
- Video Streaming over RTP/RTSP/HTTP/TCP (Media2)
- SetSynchronizationPoint (Media2)

4. Check that Security Configuration Service is supported by the DUT.

a. Check that Advanced Security Service is supported by the DUT. If **Security Configuration Service** is regarded as unsupported by the DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:

a.1. It is determined that the following features are supported by the DUT:

i. Discovery feature category:

- GetServiceCapabilities (Security Configuration)

ii. Security configuration for Signed Video feature category:

- GetCertificationPath (Security Configuration)
- GetCertificate (Security Configuration)

a.2. Check that Media Signing is supported by the DUT. If **Security Configuration Service/Media Signing** is regarded as unsupported by DUT, then it is determined that [ONVIF Media Signing 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- GetAssignedMediaSigningCertificates (Security Configuration)

6 ONVIF Profile V Security 1.0 Add-On Conformance

6.1 Feature category classification for ONVIF Profile V Security 1.0 Add-On Conformance

In order for ONVIF Device Test Tool to conduct conformance testing toward [ONVIF Profile V Security 1.0 Add-on], it would need to identify whether DUT implements the expected feature set.

This section classifies supported features as multiple categories that are related to [ONVIF Profile V Security 1.0 Add-on] conformance. Those category classifications will be used to do some preliminary checking prior to the test case execution and also they will be used to determine whether DUT can be considered to be [ONVIF Profile V Security 1.0 Add-on] conformant device.

The following discovery scope is defined as the scope that signals that DUT is [ONVIF Profile V Security 1.0 Add-on] product.

Table 6.1. ONVIF Profile V Security 1.0 Add-On Capability

ProfileVSecurity_v1

The following table shows the classified feature categories based on commands and/or functional blocks that are referenced by DUT.

Table 6.2. ONVIF Profile V Security 1.0 Add-On Conformance Features Categories

Add-on Mandatory Features	
Discovery	GetServices (Device Management)
	GetServiceCapabilities (Device Management)
	GetServiceCapabilities (Security Configuration)
	GetServiceCapabilities (Recording)
Security Configuration	CreateRSAKeyPair (Security Configuration)
	CreateECCKeyPair (Security Configuration)
	GetKeyStatus (Security Configuration)
	GetAllKeys (Security Configuration)
	DeleteKey (Security Configuration)
	GetCertificate (Security Configuration)
	GetAllCertificates (Security Configuration)
	DeleteCertificate (Security Configuration)

	UploadCertificate (Security Configuration)
	CreatePKCS10CSR (Security Configuration)
	CreateCertPathValidationPolicy (Security Configuration)
	GetCertPathValidationPolicy (Security Configuration)
	GetAllCertPathValidationPolicies (Security Configuration)
	DeleteCertPathValidationPolicy (Security Configuration)
	GetAuthorizationServerConfigurations (Security Configuration)
	CreateAuthorizationServerConfiguration (Security Configuration)
	SetAuthorizationServerConfiguration (Security Configuration)
	DeleteAuthorizationServerConfiguration (Security Configuration)
	OAuthClientCredentials (Security Configuration)
	client_secret_basic (Security Configuration)
	private_key_jwt (Security Configuration)
	MaximumNumberOfKeys >= 4 (Security Configuration)
	MaximumNumberOfCertificates >= 32 (Security Configuration)
	MaximumNumberOfCertification PathValidationPolicies >= 4 (Security Configuration)
Recording Encryption Configuration	GetRecordingOptions (Recording)
	GetRecordings (Recording)
	GetRecordingConfiguration (Recording)
	CreateRecording (Recording)
	SetRecordingConfiguration (Recording)
	Symmetric recording content encryption using CENC (Recording)

	Asymmetric recording key encryption using RSA public key (Recording)
	Asymmetric recording key encryption using ECC public key (Recording)

6.2 ONVIF Profile V Security 1.0 Add-on Support Check

Preliminary checking for feature discovery will be performed prior to the test execution. For the details of the preliminary feature discovery, refer to [ONVIF Feature Discovery].

According to the result of feature discovery execution, final determination of [ONVIF Profile V Security 1.0 Add-on] support toward DUT is performed based on the following procedure.

After this test cases required for the features determinate at feature discovery will be executed.

Procedure:

1. Check that Addons list capability contains item with equal to given in [Table 6.1](#).

If there is no such item at Addons list capability of the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported and other steps will be skipped.

2. Check Device Management Service related features:

2.1. The following features are supported by the DUT, because these are mandatory features for any ONVIF device implementation:

- i. Discovery feature category:

- GetServices (Device Management)
- GetServiceCapabilities (Device Management)

3. Check that Advanced Security Service is supported by the DUT. If **Security Configuration Service** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:

3.1. It is determined that the following features are supported by the DUT:

- i. Discovery feature category:

- GetServiceCapabilities (Security Configuration)

- ii. Security Configuration feature category:

- GetKeyStatus (Security Configuration)

- GetAllKeys (Security Configuration)
- DeleteKey (Security Configuration)
- GetCertificate (Security Configuration)
- GetAllCertificates (Security Configuration)
- DeleteCertificate (Security Configuration)
- UploadCertificate (Security Configuration)
- CreateCertPathValidationPolicy (Security Configuration)
- GetCertPathValidationPolicy (Security Configuration)
- GetAllCertPathValidationPolicies (Security Configuration)
- GetAllCertPathValidationPolicies (Security Configuration)
- DeleteCertPathValidationPolicy (Security Configuration)

3.2. Check that RSA Key Pair Generation is supported by the DUT. If **Security Configuration Service/Key Pair Generation/RSA** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- CreateRSAKeyPair (Security Configuration)

3.3. Check that ECC Key Pair Generation is supported by the DUT. If **Security Configuration Service/Key Pair Generation/ECC** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- CreateECKKeyPair (Security Configuration)

3.4. Check that PKCS#10 Requests Creation is supported by the DUT. If **Security Configuration Service/PKCS10 External Certification** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not

supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- CreatePKCS10CSR (Security Configuration)

3.5. Check that Authorization Server Configurations is supported by the DUT. If **Security Configuration Service/Authorization Server Configurations** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

3.5.1. It is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- GetAuthorizationServerConfigurations (Security Configuration)
- CreateAuthorizationServerConfiguration (Security Configuration)
- SetAuthorizationServerConfiguration (Security Configuration)
- DeleteAuthorizationServerConfiguration (Security Configuration)

3.5.2. Check that OAuth2 Client Credentials flow is supported by the DUT. If **Security Configuration Service/Authorization Server Configurations/Configuration Types/OAuth2 Client Credentials** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- OAuthClientCredentials (Security Configuration)

3.5.3. Check that client_secret_basic client authentication method is supported by the DUT. If **Security Configuration Service/Authorization Server Configurations/Client Authentication Methods/Client Secret Basic** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- client_secret_basic (Security Configuration)

3.5.4. Check that private_key_jwt client authentication method is supported by the DUT. If **Security Configuration Service/Authorization Server Configurations/Client Authentication Methods/Private Key JWT** is regarded as unsupported by DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- private_key_jwt (Security Configuration)

3.6. Check that DUT supports at least 32 key pairs. If **Security Configuration Service/GetServiceCapabilities/MaximumNumberOfKeys capability** has value less than 32, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- MaximumNumberOfKeys ≥ 4 (Security Configuration)

3.7. Check that DUT supports at least 32 certificates. If **Security Configuration Service/GetServiceCapabilities/MaximumNumberOfCertificates capability** has value less than 32, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- MaximumNumberOfCertificates ≥ 32 (Security Configuration)

3.8. Check that DUT supports at least 4 certification validation policies. If **Security Configuration Service/GetServiceCapabilities/MaximumNumberOfCertificationPathValidationPolicies capability** has value less than 4, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by DUT and certification will be FAILED. Otherwise, it is determined that the following features are supported by the DUT:

i. Security Configuration feature category:

- MaximumNumberOfCertificationPathValidationPolicies >= 4 (Security Configuration)
4. Check that Recording Control Service is supported by the DUT. If **Recording Control Service** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:
- 4.1. It is determined that the following features are supported by the DUT:
- i. Discovery feature category:
 - GetServiceCapabilities (Recording)
 - ii. Recording Encryption Configuration feature category:
 - GetRecordings (Recording)
 - SetRecordingConfiguration (Recording)
 - GetRecordingConfiguration (Recording)
- 4.2. If **Recording control Service/Dynamic Recordings** is regarded as supported by the DUT, it is determined that the following features are supported by the DUT:
- i. Recording Encryption Configuration feature category:
 - CreateRecording (Recording)
- 4.3. Check that recording encryption is supported by the DUT. If **Recording Service/Recording Encryption** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:
- 4.3.1. Check that CENC encryption mode is supported by the DUT. If **Recording Service/Recording Encryption/Encryption Modes/CENC** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:
- i. Recording Encryption Configuration feature category:
 - Symmetric recording content encryption using CENC (Recording)
- 4.3.2. Check that Asymmetric Encryption is supported by the DUT. If **Recording Service/Recording Encryption/Asymmetric Encryption** is regarded as

unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:

4.3.2.1. Check that RSA encryption is supported by the DUT. If **Security Configuration Service/Key Pair Generation/RSA** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:

i. Recording Encryption Configuration feature category:

- Asymmetric recording key encryption using RSA public key (Recording)

4.3.2.2. Check that ECC encryption is supported by the DUT. If **Security Configuration Service/Key Pair Generation/ECC** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:

i. Recording Encryption Configuration feature category:

- Asymmetric recording key encryption using ECC public key (Recording)

4.4. Check that recording options is supported by the DUT. If **Recording Service/Recording Options** is regarded as unsupported by the DUT, then it is determined that [ONVIF Profile V Security 1.0 Add-on] is not supported by the DUT and certification will be FAILED. Otherwise:

i. Recording Job Configuration feature category:

- GetRecordingOptions (Recording)