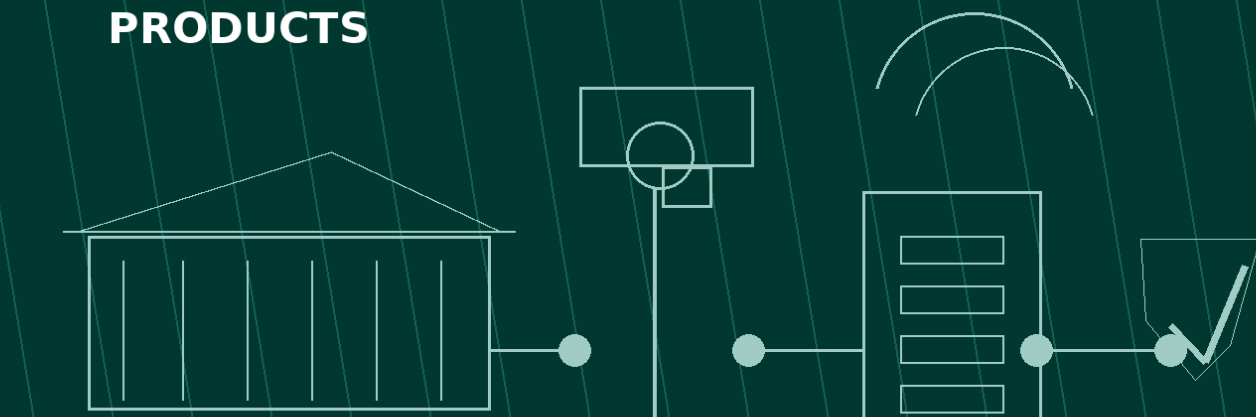


ACTi

Physical Security End-to-End Solution Provider

White Paper | ONVIF Conformant Products

ONVIF CONFORMANT PRODUCTS



A practical white paper for specifying multi-vendor video surveillance, profile-based interoperability, and audit-ready integration workflows.

Contents

- 1 Executive Summary
- 2 About ACTi Corporation
- 3 Definition of ONVIF Conformant Products
- 4 Core Technical Concepts
- 5 High-Value Applications
- 6 System Architecture
- 7 ACTi Product Portfolio Overview
- 8 Related Keywords and Terminology

Document purpose

This white paper explains what ONVIF Conformant Products mean for professional video surveillance projects, why profile-based interoperability matters, and how system integrators, consultants, and end users should specify multi-vendor video systems without reducing the requirement to a generic protocol checkbox.

It is written for project teams that need IP cameras, encoders, recording platforms, video management software, central monitoring, analytics metadata, access-control video verification, and related security systems for government, education, transportation, utilities, healthcare, enterprise, retail, and industrial environments.

The document references ACTi public product information for ONVIF conformant security product categories and official ONVIF information about profiles, conformance, and the conformant product database. It avoids model-specific naming so the content remains usable as product generations change.

Reading guide

Use Sections 3 and 4 to define ONVIF conformance and technical concepts, Section 5 to map high-value applications, Section 6 to review architecture, Section 7 to align ACTi product categories with project needs, and Section 8 to collect common terminology for tender writing and stakeholder alignment.

1. Executive Summary

ONVIF Conformant Products are devices or clients that have completed the ONVIF conformance process for one or more defined ONVIF profiles. In surveillance projects, this matters because cameras, encoders, VMS clients, NVRs, analytics services, and integration platforms must exchange video, configuration, events, metadata, storage, and control functions predictably across brands.

ONVIF states that its mission is to provide and promote standardized interfaces for effective interoperability of IP-based physical security products and services. ONVIF profiles identify fixed feature sets that conformant devices and clients must support, and official conformance must be verified through the ONVIF conformant products database. [2][3][4]

ACTi public materials describe ONVIF conformant ACTi security camera products that are listed on the official ONVIF website and positioned for integration with third-party video management systems and access control platforms. ACTi also highlights broad feature coverage such as high resolution, optical zoom, IR distance, high frame rate modes, PTZ categories, hemispheric and multi-imager categories, analytics, and specialized environmental camera categories. [1]

Core message

ONVIF conformance creates value when profile selection, official database verification, secure network design, VMS/NVR compatibility testing, evidence workflow, and lifecycle maintenance are specified together.

Key takeaways

- ONVIF conformance is profile-based; teams should specify the required profile and functional outcome, not only the word ONVIF.
- Official database verification matters because conformance is tied to product firmware or software version and submitted documentation. [4]
- Profile T is typically relevant for advanced video streaming, including H.264/H.265, imaging settings, events, metadata streaming, HTTPS streaming, PTZ-related functions, I/O, and bidirectional audio when supported. [7]
- Profile G is relevant when edge storage, recording configuration, retrieval, audio, and metadata streams are part of the design. [6]
- Profile M is relevant when analytics metadata, object classification, recognition events, geolocation, MQTT, or IoT-related metadata exchange are required. [8]
- A conformant product can still fail a project if profile scope, firmware version, cybersecurity controls, network design, storage, time synchronization, or acceptance testing are incomplete.

Procurement principle

Do not specify ONVIF only as a broad compatibility label. Specify the required profile, product category, firmware or software version, integration use case, video performance, recording policy, cybersecurity baseline, acceptance test, documentation package, and replacement rules together.

2. About ACTi Corporation

ACTi Corporation is the writer and publisher of this document. ACTi is a Taiwan-based international company founded in 2003 and serving customers in more than 100 countries. ACTi states that it has more than 20 years of experience in the security industry and has been a pioneer in video-based security technology development and innovation. [9]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem covers video surveillance, access control, control center operation, system management, system health management, AI-enabled video technologies, and third-party integration. [9]

This broader ecosystem matters for ONVIF projects. Procurement teams may begin with a camera profile requirement, but the project succeeds only when the full system maintains usable live view, reliable recording, correct event handling, searchable playback, evidence export, and maintainable integration throughout the lifecycle.

Why ACTi is relevant to ONVIF interoperability projects

ACTi strength	Project relevance
Taiwan-based security manufacturer	ACTi product planning and documentation can support security project workflows that require clear product categories, integration evidence, and regional deployment support.
End-to-end security system scope	Cameras, recording platforms, video management, access control, CMS, analytics, mobile operation, and system health management can be planned as one security architecture.
Video as a foundation	Interoperability is valuable only when the system also captures usable evidence, protects video data, supports investigation, and maintains recording reliability.
Project and documentation fit	System integrators can align product categories, ONVIF profile scope, cybersecurity settings, accessory needs, maintenance responsibilities, and acceptance documentation.

3. Definition of ONVIF Conformant Products

ONVIF Conformant Products are physical security devices, clients, or services that support at least one ONVIF profile and have completed the required conformance process. In video surveillance, this commonly relates to cameras, video encoders, video management software, recorders, analytics services, and integration platforms that need standardized interfaces for video streaming, control, events, storage, and metadata.

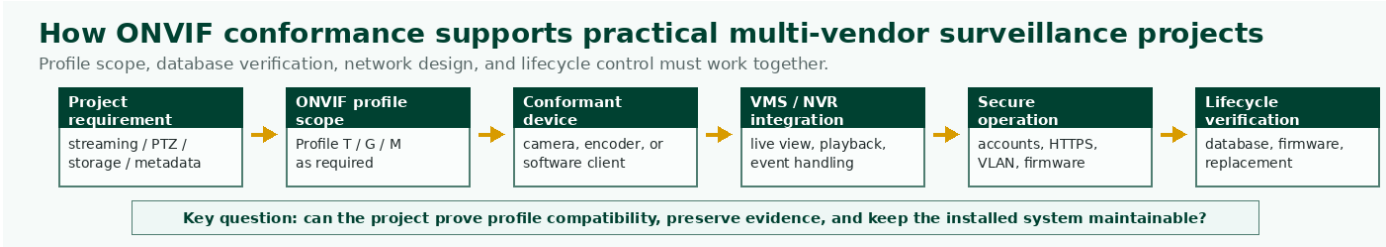
ONVIF explains that profiles make it easier to recognize compatibility between ONVIF conformant devices and clients. A profile has a fixed set of features that must be supported by conformant products, and only registered products with profile conformance are considered ONVIF conformant. [3]

The ONVIF conformant product database is the authoritative source for determining official conformance and supported profiles. ONVIF also notes that conformance is tied to the specific firmware or software version listed in the database. [4]

Conformance vs. related project concepts

Term	Meaning	Common misunderstanding
ONVIF conformant product	A registered device, client, or service that has passed the relevant ONVIF test tool and submitted the required documents.	It is not the same as simply supporting some ONVIF APIs or using a compatible stream URL.
ONVIF profile	A defined feature set that indicates how devices and clients should interoperate for a given function area.	The required profile must match the use case; one profile does not cover every possible function.
Firmware/software version	The tested version associated with official conformance and database listing.	A later or earlier firmware version should not be assumed conformant without checking the database.
Client integration	VMS, NVR, CMS, access control, or analytics platform behavior when working with a conformant device.	ONVIF conformance reduces integration risk but does not replace project acceptance testing.
Cybersecurity deployment	Secure accounts, HTTPS/TLS where applicable, VLANs, firewall policy, NTP, firmware control, logs, and remote access control.	ONVIF conformance does not automatically prove compliance with every local regulation or cybersecurity requirement. [3]

Visual Concept



Design note

ONVIF conformance creates the most value when profile review is tied to practical system design. The complete chain must be planned: tender requirement, profile selection, official database verification, camera category, field of view, PoE/network path, cybersecurity policy, recording platform, VMS/NVR search, evidence export, firmware maintenance, asset inventory, and replacement control.

Practical deployment interpretation

In a school, courthouse, smart building, hospital, transportation site, utility facility, manufacturing campus, warehouse, retail chain, or public service center, the system may face multi-vendor integration needs, privacy concerns, difficult lighting, remote monitoring, long retention, analytics events, cybersecurity review, and future replacement needs. The design should protect both interoperability confidence and operational evidence value.

4. Core Technical Concepts

ONVIF Conformant Product projects should begin with the intended integration outcome, the profile requirement, and the target operating environment. The goal is not only to select products that can communicate; it is to build a surveillance system that provides predictable live view, control, recording, event handling, metadata exchange, and evidence workflows across components.

Concept	Practical meaning
Profile scope	Identify whether the project requires Profile T for advanced video streaming, Profile G for recording and retrieval, Profile M for analytics metadata and events, or additional profiles for access-control use cases.
Official verification	Check the ONVIF conformant product database for product name, profile, application type, tested firmware or software version, Declaration of Conformance, FeatureList, and Interface Guide. [4]
Device-client pairing	Match camera, encoder, VMS, NVR, CMS, analytics service, and access-control platform behavior to the same profile and functional requirements.
Streaming and media	Define codec, resolution, frame rate, stream count, multicast need, PTZ control, audio, imaging settings, metadata stream, and HTTPS streaming where applicable.
Events and metadata	Define whether motion, tampering, digital input, relay output, analytics metadata, object classification, recognition events, or MQTT interfaces are required.
Cybersecurity controls	Plan password policy, role control, HTTPS/TLS where supported, VLANs, firewalls, time synchronization, remote access control, firmware workflow, and audit records.
Acceptance and lifecycle	Test live view, playback, search, export, failover behavior, event actions, retention, logs, firmware version, replacement rules, and handover documentation.

Specification interpretation

A product can appear compatible but still fail the project if the wrong profile is specified, a firmware version differs from the database record, the VMS uses a limited integration driver, PTZ control is untested, metadata is not mapped, time is not synchronized, or exported evidence cannot be reproduced during an investigation. Conversely, a well-integrated system can improve interoperability, evidence value, operational efficiency, and replacement control at the same time.

Capability Matrix

Project requirement	What can go wrong	Capabilities to specify	Operational output
Multi-vendor procurement	Products claim ONVIF support but do not match the required profile or official database record.	Profile requirement, database check, firmware/software version, DoC, Interface Guide, FeatureList.	Defensible procurement and smoother acceptance review.
VMS/NVR integration	Live view works, but PTZ, events, audio, metadata, playback, or export do not behave as expected.	Integration test plan, client profile support, stream settings, event mapping, playback/export checklist.	Reliable operation across vendors and fewer site-level surprises.
Evidence and privacy	Video is recorded, but timestamps, access rights, retention, or export logs are not investigation-ready.	Retention policy, NTP, user permissions, export control, watermark/log policy, evidence SOP.	Searchable, attributable, and usable evidence.
Analytics and metadata	People, vehicle, license plate, or object metadata is generated but not consumable by the client system.	Profile M scope, metadata stream, event service, rule configuration, analytics test cases.	More usable event search, filtering, and operator response.
Long-term lifecycle	Products are replaced or firmware is upgraded without checking profile conformance and integration behavior.	Replacement rule, database recheck, firmware record, compatibility review, handover package.	Maintainable interoperability over the system lifecycle.

How to use this matrix

Use the matrix during site survey and proposal design. Each procurement requirement should be translated into a profile requirement, product category, database verification step, client integration requirement, network security requirement, recording requirement, maintenance requirement, and audit documentation requirement.

For tender writing, define the project type first. Then specify the ONVIF profile scope, product categories, firmware/software version control, video performance, cybersecurity baseline, recording platform, evidence export process, replacement rules, and documentation package.

5. High-Value Applications

ONVIF Conformant Products are most valuable where project teams need predictable interoperability across devices, clients, recorders, analytics services, access control, and enterprise security workflows. ACTi public materials connect ONVIF conformant product categories with third-party VMS and access control integration, while ONVIF defines profiles that support video, storage, metadata, and access-control use cases. [1][3]

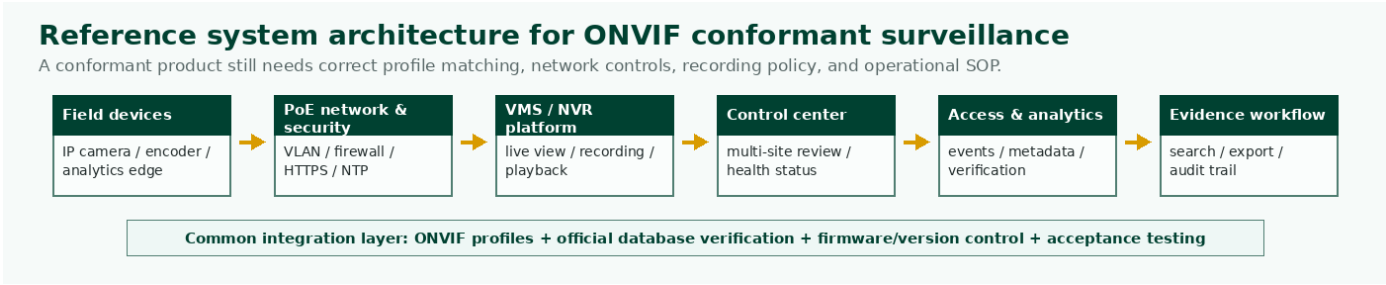
Application	Operational value	Typical locations
Government and public facilities	Support multi-vendor procurement, public-area monitoring, perimeter review, incident investigation, and audit records.	City halls, courthouses, public service centers, administrative buildings.
Schools and campuses	Align camera procurement with VMS compatibility, student safety, privacy expectations, searchable evidence, and network policy.	Entrances, corridors, parking areas, dormitories, campus perimeters.
Utilities and critical infrastructure	Enable consistent device integration while monitoring restricted zones, operational assets, and perimeter threats.	Power facilities, water plants, substations, data centers, control rooms.
Transportation and airports	Support high-traffic monitoring, restricted-area surveillance, PTZ operation, playback, and evidence workflows.	Stations, terminals, depots, platforms, parking, service areas.
Healthcare facilities	Protect public areas and staff-only spaces while respecting access control, privacy, and evidence retention needs.	Hospitals, clinics, laboratories, care facilities.
Corporate and industrial sites	Meet customer-imposed interoperability requirements while supporting operations, safety, investigation, and replacement control.	Offices, warehouses, factories, logistics yards, R&D labs.

Value by stakeholder

Stakeholder	Main benefit
System integrator	Stronger differentiation when proposals connect profile evidence, secure architecture, recording, documentation, and lifecycle support.
Consultant	Clearer specification language for profile scope, integration controls, evidence retention, and audit documents.
Security manager / operator	Reliable live view, event search, playback, export, and health visibility without reducing the project to a protocol checkbox.
Procurement team	A more defensible buying decision based on official conformance evidence, application fit, support risk, lifecycle cost, and replacement control.

6. System Architecture

ONVIF Conformant Product projects should be designed as system architecture. The camera provides the field video source, but the full solution must preserve operational value through mounting, power, network, cybersecurity, recording, live viewing, playback, search, export, notification, health monitoring, documentation, and maintenance workflow.



Architecture layers

Layer	Role in ONVIF conformant surveillance
Field layer	Camera location, form factor, lens, image quality, lighting, IR, WDR, audio if needed, enclosure, mounting, vandal resistance, and environmental protection.
Network layer	PoE, switching, VLANs, latency, HTTPS/TLS where supported, firewall rules, time synchronization, surge protection, and cyber controls.
Interoperability layer	ONVIF profile scope, database verification, firmware/software version, DoC, Interface Guide, FeatureList, and acceptance test records.
Recording layer	NVR or VMS storage, codec, bit rate, frame rate, retention, snapshots, bookmarks, playback, search, export, and evidence workflow.
Management layer	Client software, web access, CMS, mobile client, user permissions, event review, multi-site monitoring, notification policy, and health management.
Response layer	Operator SOP, incident review, escalation, maintenance ticketing, evidence export, audit trail, and decommissioning process.

Architecture warning

A camera system can still underperform if the field of view is wrong, profile scope is incomplete, network controls are weak, time is not synchronized, the recorder uses the wrong profile, retention is insufficient, health alarms are ignored, or conformance documentation is not kept current.

7. ACTi Product Portfolio Overview

ACTi positions its ONVIF conformant product portfolio around broad surveillance needs, including camera categories and integration-relevant features listed on its public page. ACTi states that its ONVIF conformant products are listed on the official ONVIF website and are intended to support integration with third-party video management systems and access control platforms. [1]

This section intentionally describes product categories and form factors rather than specific model names so the white paper remains usable as individual product generations and part numbers change.

Portfolio categories

Category	Where it fits	Use-case fit
Fixed dome, bullet, turret, and box cameras	General indoor/outdoor coverage where clear video, stable recording, and profile-based interoperability are required.	Entrances, corridors, parking areas, perimeters, offices, schools.
PTZ and high-zoom cameras	Large-area monitoring where operators need optical zoom, directional control, and long-distance verification.	Campuses, utilities, ports, airports, logistics yards, city surveillance.
Fisheye and multi-imager cameras	Wide-area coverage where fewer camera positions must monitor broad scenes or intersections.	Lobbies, warehouses, intersections, open halls, large rooms.
Special environment cameras	Harsh or specialized sites requiring higher durability, environmental resistance, or special protection.	Coastal areas, industrial sites, hazardous environments, transportation, utilities.
NVR/VMS/CMS and analytics ecosystem	Recording, live view, playback, investigation, multi-site monitoring, event review, and system operation.	Control rooms, security operations centers, distributed facilities.

Portfolio-level capabilities to confirm

- Required ONVIF profile, product category, indoor/outdoor installation, lens, resolution, WDR, low-light, IR, zoom, frame rate, and analytics needs.
- Official database record, firmware/software version, Declaration of Conformance, FeatureList, Interface Guide, and customer-specific clauses.
- Recorder/VMS compatibility, codec, retention, synchronized time, search, playback, export, CMS, remote access, and health monitoring.
- Cybersecurity requirements such as secure transmission, account control, password policy, firmware policy, network segmentation, and remote access.
- Accessory compatibility, cabling, PoE budget, mounting, environmental protection, installation space, maintenance access, and service workflow.

Project note

Product availability, detailed specifications, conformance status, integration scope, accessory compatibility, recorder compatibility, and regional part numbers should be confirmed from the latest ACTi product pages, official ONVIF database records, datasheets, release notes, installation guides, and quotation documents before project submission.

8. Related Keywords and Terminology

The following keyword reference groups collect common terms related to ONVIF Conformant Products, profile-based interoperability, video surveillance architecture, cybersecurity, evidence management, and project planning.

Core topic keywords

ONVIF Conformant Products, ONVIF conformant camera, ONVIF conformant device, ONVIF profile, profile-based interoperability, multi-vendor surveillance, IP camera interoperability, video surveillance integration, open security standard, physical security interoperability

ONVIF profile keywords

Profile T, Profile S, Profile G, Profile M, Profile A, Profile C, Profile D, ONVIF add-on, TLS Configuration Add-on, ONVIF Device Test Tool, ONVIF Client Test Tool, Declaration of Conformance, Interface Guide, FeatureList

Camera and hardware keywords

IP camera, video encoder, dome camera, bullet camera, turret camera, box camera, PTZ camera, fisheye camera, multi-imager camera, thermal camera, anti-corrosion camera, explosion-protected camera, PoE camera, edge analytics camera

Streaming and media keywords

H.264, H.265, RTSP, HTTPS streaming, media profile, video stream, metadata stream, audio input, bidirectional audio, multicast, imaging settings, PTZ control, motion alarm, tampering event, digital input, relay output

Software and integration keywords

VMS integration, NVR recording, CMS monitoring, video playback, edge storage, evidence export, event search, metadata mapping, access control video verification, mobile client, notification workflow, system health management, asset inventory

Cybersecurity control keywords

HTTPS, TLS, VLAN, firewall, password policy, account management, role-based access control, time synchronization, secure firmware, remote access control, device hardening, network segmentation, audit log

Application keywords

government facility surveillance, school security cameras, utility site monitoring, airport surveillance, transit security, hospital security cameras, critical infrastructure security, corporate compliance surveillance, warehouse security, perimeter surveillance

Common Question Phrases

what are ONVIF Conformant Products, what is an ONVIF profile, how to specify ONVIF conformant cameras, how to verify ONVIF conformance, how to check the ONVIF database, how to choose between Profile T and Profile S, when to specify Profile G, when to specify Profile M, how to integrate ONVIF cameras with VMS, how to verify ONVIF firmware version, how to test PTZ control, how to retain video evidence, how to export surveillance evidence, how to manage camera firmware, how to prepare an ONVIF acceptance test

Source notes

Ref.	Source
[1]	ACTi Corporation, "ONVIF Conformant Products," official product category page. URL: https://www.acti.com/products/onvif-conformant-products . Accessed: June 30, 2026.
[2]	ONVIF, "Our Mission," official overview page. URL: https://www.onvif.org/about/mission/ . Accessed: June 30, 2026.
[3]	ONVIF, "ONVIF Profiles," official profiles overview page. URL: https://www.onvif.org/profiles/ . Accessed: June 30, 2026.
[4]	ONVIF, "Conformant Products," official database page. URL: https://www.onvif.org/conformant-products/ . Accessed: June 30, 2026.
[5]	ONVIF, "Profile S," official profile page. URL: https://www.onvif.org/profiles/profile-s/ . Accessed: June 30, 2026.
[6]	ONVIF, "Profile G," official profile page. URL: https://www.onvif.org/profiles/profile-g/ . Accessed: June 30, 2026.
[7]	ONVIF, "Profile T," official profile page. URL: https://www.onvif.org/profiles/profile-t/ . Accessed: June 30, 2026.
[8]	ONVIF, "Profile M," official profile page. URL: https://www.onvif.org/profiles/profile-m/ . Accessed: June 30, 2026.
[9]	ACTi Corporation, "About ACTi," official corporate page. URL: https://www.acti.com/corporate . Accessed: June 30, 2026.

Revision note

Revision note

This document is a marketing and technical education white paper. It is not a legal opinion, interoperability certification, cybersecurity audit, privacy assessment, penetration test, or final project design. Always validate current ONVIF records, tender requirements, firmware/software versions, profile scope, field of view, lighting, recording settings, storage, network security, VMS control, system health monitoring, maintenance access, and operator workflow in the target scene before deployment.

Prepared by ACTi Corporation

For ONVIF Conformant Product projects, confirm product category selection, profile requirements, firmware/software version, recording platform, cybersecurity policy, mounting accessories, and regional availability with your ACTi sales contact or authorized system integrator.
sales@acti.com | www.acti.com