

AS/NZS IEC 60839.11.31:2020
IEC 60839-11-31:2016



STANDARDS
Australia

Australian/New Zealand Standard™

Alarm and electronic security systems

**Part 11.31: Electronic access control systems — Core interoperability
protocol based on Web services**



AS/NZS IEC 60839.11.31:2020

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee EL-031, Intruder Alarm Equipment and Installations. It was approved on behalf of the Council of Standards Australia on 24 September 2020 and by the New Zealand Standards Approval Board on 7 October 2020.

This Standard was published on 23 October 2020.

The following are represented on Committee EL-031:

- Australian Digital and Telecommunications Industry Association
- Australian Industry Group
- Australian Security Industry Association
- Engineers Australia
- Fire Protection Association Australia
- Insurance Council of Australia
- NSW Police Force
- New Zealand Security Association
- Security Providers Association of Australia
- South Australia Police
- Victorian Security Institute

This Standard was issued in draft form for comment as DR AS/NZS IEC 60839.11.31:2020.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

Australian/New Zealand Standard™

Alarm and electronic security systems

Part 11.31: Electronic access control systems — Core interoperability protocol based on Web services

First published as AS/NZS IEC 60839.11.31:2020.



© IEC 2020 — All rights reserved

© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2020

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee EL-031, Intruder Alarm Equipment and Installations.

The objective of this document is to define procedures for communication between network clients and devices. This series of interoperability standards makes it possible to build an alarm and electronic security system with clients and devices from different manufacturers using common and well-defined interfaces. The functions defined in this document cover discovery, device management and event framework. Supplementary dedicated services are defined in separate documents.

The management and control interfaces defined in this document are described as Web services. This document also contains full XML schema and Web Service Description Language (WSDL) definitions.

In order to offer full plug-and-play interoperability, this document defines procedures for device discovery. The device discovery mechanisms in this document are based on the Web Discovery specification with extensions.

This document does not in any way limit a manufacturer to add other protocol or extend the protocol defined here and rules on how to accomplish this are also provided in this document.

This document is identical with, and has been reproduced from, IEC 60839-11-31:2016, *Alarm and electronic security systems — Part 11-31: Electronic access control systems — Core interoperability protocol based on Web services*.

As this document has been reproduced from an International Standard, the following applies:

- (a) In the source text “this part of IEC 60839” should read “this document”.
- (b) A full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

NOTES

Currently in preview, click buy full version

CONTENTS

FOREWORD.....	10
INTRODUCTION.....	12
1 Scope.....	13
2 Normative references	13
3 Terms, definitions and abbreviated terms	15
3.1 Terms and definitions.....	15
3.2 Abbreviated terms.....	16
4 Overview	17
4.1 General.....	17
4.2 Web services	17
4.3 IP configuration.....	18
4.4 Device discovery.....	18
4.5 Device management	19
4.5.1 General	19
4.5.2 Capabilities.....	19
4.5.3 Network	19
4.5.4 System	20
4.5.5 Retrieval of system information.....	20
4.5.6 Firmware upgrade.....	20
4.5.7 SystemRestore	20
4.5.8 Security	20
4.6 DeviceIO.....	21
4.7 Event handling.....	21
4.8 Security	21
5 Web services framework.....	21
5.1 General.....	21
5.2 Services overview.....	22
5.2.1 General	22
5.2.2 Services requirements	22
5.3 WSDL overview	22
5.4 Namespaces.....	23
5.5 Types.....	24
5.6 Messages	24
5.7 Operations	25
5.7.1 General	25
5.7.2 One-way operation type.....	26
5.7.3 Request-response operation type	26
5.8 Port types	27
5.9 Binding	27
5.10 Ports.....	27
5.11 Services.....	28
5.12 Error handling	28
5.12.1 General	28
5.12.2 Protocol errors.....	28
5.12.3 SOAP errors	28
5.13 Security	31

5.13.1	Authentication.....	31
5.13.2	User-based access control	31
5.14	String representation	33
5.14.1	Character set.....	33
5.14.2	Allowed characters in strings	33
5.15	Proprietary extensions	33
6	IP configuration	33
7	Device discovery	34
7.1	General.....	34
7.2	Modes of operation	34
7.3	Discovery definitions	35
7.3.1	Endpoint reference	35
7.3.2	Hello.....	35
7.3.3	Probe and probe match	36
7.3.4	Resolve and resolve match.....	37
7.3.5	Bye.....	37
7.3.6	SOAP fault messages.....	37
8	Device management.....	37
8.1	General.....	37
8.2	Capabilities.....	38
8.2.1	Get WSDL URL	38
8.2.2	Capability exchange	38
8.3	Network	40
8.3.1	Get hostname	40
8.3.2	Set hostname	40
8.3.3	Set hostname from DHCP.....	41
8.3.4	Get DNS settings.....	41
8.3.5	Set DNS settings	42
8.3.6	Get NTP settings.....	42
8.3.7	Set NTP settings.....	43
8.3.8	Get dynamic DNS settings	43
8.3.9	Set dynamic DNS settings	44
8.3.10	Get network interface configuration	44
8.3.11	Set network interface configuration.....	45
8.3.12	Get network protocols.....	46
8.3.13	Set network protocols	47
8.3.14	Get default gateway.....	47
8.3.15	Set default gateway	48
8.3.16	Get zero configuration	48
8.3.17	Set zero configuration.....	48
8.3.18	Get IP address filter.....	49
8.3.19	Set IP address filter	49
8.3.20	Add an IP filter address	50
8.3.21	Remove an IP filter address.....	50
8.3.22	IEEE 802.11 configuration	51
8.4	System	55
8.4.1	Device information.....	55
8.4.2	Get system URIs	55
8.4.3	Backup	56

8.4.4	Restore.....	56
8.4.5	Start system restore	57
8.4.6	Get system date and time	57
8.4.7	Set system date and time	58
8.4.8	Factory default.....	59
8.4.9	Firmware upgrade.....	59
8.4.10	Start firmware upgrade	60
8.4.11	Get system logs.....	61
8.4.12	Get support information	61
8.4.13	Reboot.....	62
8.4.14	Get scope parameters	62
8.4.15	Set scope parameters.....	62
8.4.16	Add scope parameters.....	63
8.4.17	Remove scope parameters	63
8.4.18	Get discovery mode.....	64
8.4.19	Set discovery mode	64
8.5	Security	65
8.5.1	General	65
8.5.2	Get access policy	65
8.5.3	Set access policy.....	65
8.5.4	Get users.....	65
8.5.5	Create users.....	66
8.5.6	Delete users	67
8.5.7	Set users settings	67
8.5.8	IEEE 802.1X configuration.....	68
8.5.9	Create self-signed certificate	71
8.5.10	Get certificates	71
8.5.11	Get CA certificates	71
8.5.12	Get certificate status.....	72
8.5.13	Set certificate status.....	72
8.5.14	Get certificate request	72
8.5.15	Get client certificate status	73
8.5.16	Set client certificate status.....	73
8.5.17	Load device certificate.....	74
8.5.18	Load device certificates in conjunction with its private key	74
8.5.19	Get certificate information request	75
8.5.20	Load CA certificates	76
8.5.21	Delete certificate	76
8.5.22	Get remote user.....	76
8.5.23	Set remote user	77
8.5.24	Get endpoint reference	77
8.6	Auxiliary operation	78
8.7	Monitoring events	78
8.7.1	Processor usage.....	78
8.7.2	Link status	79
8.7.3	Upload status	79
8.7.4	Operating time.....	79
8.7.5	Environmental conditions.....	81
8.7.6	Battery capacity.....	81

8.7.7	Device management	82
8.8	Service specific fault codes	82
9	Device I/O	86
9.1	General	86
9.2	Relay outputs	86
9.2.1	Overview	86
9.2.2	Get relay outputs	86
9.2.3	Get relay output options	86
9.2.4	Set relay output settings	87
9.2.5	Trigger relay output	88
9.3	Digital inputs	88
9.3.1	Overview	88
9.3.2	GetDigitalInputs	88
9.4	SerialPorts	89
9.4.1	Overview	89
9.4.2	GetSerialPorts	89
9.4.3	GetSerialPortConfiguration	89
9.4.4	SetSerialPortConfiguration	89
9.4.5	GetSerialPortConfigurationOptions	90
9.4.6	Send and/or Receive serial command	90
9.5	Capabilities	92
9.6	Events	92
9.6.1	DigitalInput state change	92
9.6.2	Relay output trigger	92
9.7	Service specific fault codes	93
10	Event handling	93
10.1	General	93
10.2	Real-time Pull-Point notification interface	93
10.2.1	General	93
10.2.2	Create pull point subscription	95
10.2.3	Pull message	95
10.2.4	Renew	96
10.2.5	Unsubscribe	96
10.2.6	Seek	97
10.2.7	Pull point lifecycle	98
10.2.8	Persistent notification storage	98
10.3	Basic notification interface	98
10.3.1	General	98
10.3.2	Summary	98
10.3.3	Requirements	99
10.4	Properties	100
10.5	Notification structure	100
10.5.1	General	100
10.5.2	Notification information	101
10.5.3	Message format	102
10.5.4	Message description language	103
10.5.5	Message content filter	104
10.6	Synchronization point	105
10.7	Topic structure	105

10.7.1	General	105
10.7.2	ONVIF topic namespace	106
10.7.3	Topic type information	106
10.7.4	Topic filter	107
10.8	Get event properties	108
10.9	Capabilities	108
10.10	SOAP fault messages	109
10.11	Notification example	110
10.11.1	General	110
10.11.2	GetEventPropertiesRequest	110
10.11.3	GetEventPropertiesResponse	110
10.11.4	CreatePullPointSubscription	111
10.11.5	CreatePullPointSubscriptionResponse	111
10.11.6	PullMessagesRequest	112
10.11.7	PullMessagesResponse	112
10.11.8	UnsubscribeRequest	113
10.11.9	UnsubscribeResponse	113
10.12	Persistent storage event:BeginingOfBuffer	114
10.13	Service specific fault codes	114
11	Security	114
11.1	General	114
11.2	Transport level security	114
11.2.1	General	114
11.2.2	Supported cipher suites	115
11.2.3	Server authentication	115
11.2.4	Client authentication	115
11.3	IEEE 802.1X	116
Annex A (informative)	Example for GetServices response with capabilities	117
Annex B (normative)	Device IP network interface XML schemata	119
B.1	Device management service WSDL	119
B.2	Device IO service WSDL	161
B.3	Event service WSDL	168
B.4	Common schema	179
Bibliography		197
Figure 1	– Web services based development principles	18
Figure 2	– Sequence diagram for the Real-time Pull-Point notification interface	94
Figure 3	– Sequence diagram for the base notification interface	99
Table 1	– Defined namespaces in this document	23
Table 2	– Referenced namespaces (with prefix)	24
Table 3	– Referenced namespaces (without prefix)	24
Table 4	– Operation description outline used in this document	25
Table 5	– Generic faults	30
Table 6	– HTTP errors	31
Table 7	– Access class to user level mapping	32
Table 8	– Scope parameters	36

Table 9 – GetWSDLUrl command.....	38
Table 10 – GetServices command.....	38
Table 11 – GetServiceCapabilities command	39
Table 12 – Capabilities in the GetServiceCapabilities command	39
Table 13 – GetHostname command	40
Table 14 – SetHostname command.....	41
Table 15 – SetHostnameFromDHCP command	41
Table 16 – GetDNS command.....	42
Table 17 – SetDNS command	42
Table 18 – GetNTP command	43
Table 19 – SetNTP command	43
Table 20 – GetDynamicDNS command	44
Table 21 – SetDynamicDNS command.....	44
Table 22 – GetNetworkInterfaces command	45
Table 23 – SetNetworkInterfaces command	46
Table 24 – GetNetworkProtocols command.....	47
Table 25 – SetNetworkProtocols command	47
Table 26 – GetNetworkDefaultGateway command.....	47
Table 27 – SetNetworkDefaultGateway command	48
Table 28 – GetZeroConfiguration command	48
Table 29 – SetZeroConfiguration command	49
Table 30 – GetIPAddressFilter command	49
Table 31 – SetIPAddressFilter command	50
Table 32 – AddIPAddressFilter command	50
Table 33 – RemoveIPAddressFilter command.....	51
Table 34 – GetDot11Capabilities.....	53
Table 35 – IEEE 802.11 capabilities.....	53
Table 36 – GetDot11Status.....	54
Table 37 – ScanAvailableDot11Networks	55
Table 38 – GetDeviceInformation command	55
Table 39 – GetSystemUri command	56
Table 40 – GetSystemBackup command	56
Table 41 – RestoreSystem command	57
Table 42 – StartSystemRestore command	57
Table 43 – GetSystemDateAndTime command	58
Table 44 – SetSystemDateAndTime command.....	59
Table 45 – SetSystemFactoryDefault command	59
Table 46 – UpgradeSystemFirmware command	60
Table 47 – StartFirmwareUpgrade command	60
Table 48 – GetSystemLog command.....	61
Table 49 – GetSystemSupportInformation command	61
Table 50 – SystemReboot command	62
Table 51 – GetScopes command	62

Table 52 – SetScopes command	63
Table 53 – AddScopes command	63
Table 54 – RemoveScopes command	64
Table 55 – GetDiscoveryMode command	64
Table 56 – SetDiscoveryMode command	64
Table 57 – GetAccessPolicy command	65
Table 58 – SetAccessPolicy command	65
Table 59 – GetUsers command	66
Table 60 – CreateUsers command	66
Table 61 – DeleteUsers command	67
Table 62 – SetUser command	67
Table 63 – CreateDot1XConfiguration command	69
Table 64 – SetDot1XConfigurationRequest command	69
Table 65 – GetDot1XConfiguration command	70
Table 66 – GetDot1XConfigurations command	70
Table 67 – DeleteDot1XConfigurations command	70
Table 68 – CreateCertificate command	71
Table 69 – GetCertificates command	71
Table 70 – GetCACertificates command	72
Table 71 – GetCertificatesStatus command	72
Table 72 – SetCertificatesStatus command	72
Table 73 – GetPkcs10Request command	73
Table 74 – GetClientCertificateMode command	73
Table 75 – SetClientCertificateMode command	74
Table 76 – LoadCertificates command	74
Table 77 – LoadCertificateWithPrivateKey command	75
Table 78 – GetCertificateInformation command	75
Table 79 – LoadCACertificates command	76
Table 80 – DeleteCertificates command	76
Table 81 – GetRemoteUser command	77
Table 82 – SetRemoteUser command	77
Table 83 – GetEndpointReference command	78
Table 84 – SendAuxiliary command	78
Table 85 – Device service specific fault codes	82
Table 86 – GetRelayOutputs command	86
Table 87 – GetRelayOutputOptions command	87
Table 88 – SetRelayOutputSettings command	88
Table 89 – SetRelayOutputState command	88
Table 90 – GetDigitalInputs command	89
Table 91 – GetSerialPorts command	89
Table 92 – GetSerialPortConfiguration command	89
Table 93 – SetSerialPortConfiguration command	90
Table 94 – GetSerialPortConfigurationOptions command	90

Table 95 – Send and/or Receive serial command.....	91
Table 96 – GetServiceCapabilities command	92
Table 97 – DeviceIO service specific fault codes	93
Table 98 – CreatePullPointSubscription command	95
Table 99 – PullMessages command	96
Table 100 – Renew command	96
Table 101 – Unsubscribe command	97
Table 102 – Seek command.....	97
Table 103 – SetSynchronizationPoint command.....	105
Table 104 – GetEventProperties command	108
Table 105 – GetServiceCapabilities command	109

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM AND ELECTRONIC SECURITY SYSTEMS –**Part 11-31: Electronic access control systems –
Core interoperability protocol based on Web services**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60839-11-31 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

The text of this standard is based on the following documents:

CDV	Report on voting
79/522/CDV	79/546/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 60839 series, published under the general title *Alarm and electronic security systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The object of this document is to provide the common base for a fully interoperable network implementation comprised of products from different network vendors. This document describes the network model, interfaces, data types and data exchange patterns. This document reuses existing relevant standards where available, and introduces new specifications only where necessary.

This document is based upon work done by the ONVIF open industry forum. The ONVIF Core specification is compatible with this document.

This document is accompanied by a set of computer readable interface definitions:

- Device Service WSDL, see Clause B.1;
- Device IO Service WSDL, see Clause B.2;
- Event Service WSDL, see Clause B.3;
- Common schema, see Clause B.4.

This document is divided into the following clauses:

Document overview: Gives an overview of the different standard parts and how they are related to each other.

Web services frame work: Offers a brief introduction to Web services and the Web services basis for this document.

IP configuration: Defines the network IP configuration requirements.

Device discovery: Describes how devices are discovered in local and remote networks.

Device management: Defines the configuration of basics like network and security related settings.

Device IO: Defines the handling of input and output ports on a device.

Event handling: Defines how to subscribe to and receive notifications (events) from a device.

Security: Defines the transport and message level security requirements.

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-31: Electronic access control systems – Core interoperability protocol based on Web services

1 Scope

This part of IEC 60839 defines procedures for communication between network clients and devices. This series of interoperability standards makes it possible to build an alarm and electronic security system with clients and devices from different manufacturers using common and well defined interfaces. The functions defined in this document covers discovery, device management and event framework. Supplementary dedicated services are defined in separate documents.

The management and control interfaces defined in this document are described as Web services. This document also contains full XML schema and Web Service Description Language (WSDL) definitions.

In order to offer full plug-and-play interoperability, this document defines procedures for device discovery. The device discovery mechanisms in this document are based on the WS-Discovery specification with extensions.

This document does not in any way limit a manufacturer to add other protocol or extend the protocol defined here and rules on how to accomplish this are also provided in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEEE 1003.1, *The Open Group Base Specifications Issue 6, IEEE Std 1003.1, 2004 Edition*
<<http://pubs.opengroup.org/onlinepubs/009695399/>>

IEEE 802.11, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*
<<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>>

IEEE 802.1X, *Port-Based Network Access Control*
<<http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>>

IETF RFC 952, *Internet Host Table Specification*
<<https://tools.ietf.org/html/rfc952>>

IETF RFC 1123:1989, *Requirements for Internet Hosts – Application and Support*
<<https://tools.ietf.org/html/rfc1123>>

IETF RFC 2131, *Dynamic Host Configuration Protocol*
<<http://www.ietf.org/rfc/rfc2131.txt>>

IETF RFC 2136, *Dynamic Updates in the Domain Name System (DNS UPDATE)*
<<http://www.ietf.org/rfc/rfc2136.txt>>