

App-IDs for ICS and SCADA

Support for Industrial Control Systems
Protocols and Applications

Overview

This document is a listing of application identifiers, or App-IDs, supported by App-ID technology on Palo Alto Networks ML-Powered Next-Generation Firewalls for applications and protocols used to support operational technology (OT) industrial control systems (ICS). The list includes applications and protocols from the internet of things (IoT), industrial internet of things (IIoT), and cellular protocols. It is broken up into four sections as follows:

- App-IDs with base-level variants
- App-IDs with base- and function-level variants
- Decoders for creating custom, function-level App-IDs
- Submitting new App-ID requests

Note that new App-IDs for ICS are being added on a regular basis. If your protocol/application of interest is not covered in this document, make sure to check the Palo Alto Networks Applipedia data-base for the most current information on App-IDs. Visit <https://applipedia.paloaltonetworks.com>.

Supported Base ICS App-IDs

The following base ICS App-IDs are available in Applipedia.

Table 1: Base ICS App-IDs	
104 APCI	KNXNET/IP
ABB Network Manager	Lenel Intelligent System Controller
ABB-RP570	Matrikon-tunneller
ADDP	Meteorological Archival & Retrieval Systems (MARS)
BACnet	Mitsubishi-melsec
CC-Link	MMS-ICS
CIP EtherNet IP	Modbus
CN/IP (CEA-852)	MQTT
COAP	MTConnect
Cygnat SCADA	Net-C-X
DLMS / COSEM / IEC 62056	Niagara-Fox
DNP3	Oasys-scada
Elcom 90	Omron-fins
Emerson-Delta-V	OPC-DA
Ethercat	OPC UA
Ether-S-Bus	OSisoft PI Systems
ETHER-S-I/O (esio)	Ovation
Fanuc-focas	Profinet
Fisher-ROC	R-GOOSE
Foundation Fieldbus	ROC
GE EGD	Rockwell-Factorytalk-Viewpoint
GE-Eterra-isd	RTCM (GPS/IP)
GE-Eterra-SCADA	RTPS
GE-Historian	Schneider Electric Square-D-Discovery
GE iFIX	Schneider OASyS
HDLC-OVER-TCP	Schneider Wonderware Suitelink
Honeywell Matrikon OPC Tunneller	Schweitzer Engineering SEL Fast Messaging
Honeywell-Pro-Watch	Siemens FactoryLink
IEEE-c37.118-Synchrophasor	Siemens Profinet IO
Ingenico-pos	Siemens-P2
IRIG-106	Siemens S7
ICCP (IEC 60870-6 / TASE.2)	Siemens S7-Comm-Plus
IEC 60870-5-104	Suitelink
IEC-61850	Twincat
Johnson-Controls-Metasys	

Table 2: Base IoT/IIoT
Advance Messaging Queuing Protocol (AMQP)
RabbitMQ

Table 3: Base Cellular
General Packet Radio Service (GPRS)
Signal System 7 (SS7)

ICS App-IDs with Function-Level Variants

Several App-IDs, in addition to a base identifier, also have function-level variants to allow more granular visibility and precise control. These are listed below.

Table 4: Modbus
modbus-base
modbus-encapsulated-transport
modbus-mask-write-register
modbus-read-coils
modbus-read-discrete-inputs
modbus-read-fifo-queue
modbus-read-file-record
modbus-read-holding-registers
modbus-read-input-registers
modbus-read-write-register
modbus-write-file-record
modbus-write-multiple-coils
modbus-write-multiple-registers
modbus-write-single-coil
modbus-write-single-register

Table 5: CIP-EtherNet-IP

cip-ethernet-ip-base
 cip-ethernet-ip-disable-io (functional)
 cip-ethernet-ip-disable-sfc (functional)
 cip-ethernet-ip-enable-io (functional)
 cip-ethernet-ip-enable-sfc (functional)
 cip-ethernet-ip-list-identity (functional)
 cip-ethernet-ip-read-mod-write (functional)
 cip-ethernet-ip-read-tag (functional)
 cip-ethernet-ip-read-tag-frag (functional)
 cip-ethernet-ip-reg-session (functional)
 cip-ethernet-ip-run (functional)
 cip-ethernet-ip-send-rr-data (functional)
 cip-ethernet-ip-send-unit-data (functional)
 cip-ethernet-ip-stop (functional)
 cip-ethernet-ip-test-mode (functional)
 cip-ethernet-ip-write-tag (functional)
 cip-ethernet-ip-write-tag-frag (functional)

Table 6: DNP3

dnp3-abort-file
 dnp3-assign-class
 dnp3-authenticate-file
 dnp3-base
 dnp3-close-file
 dnp3-cold-restart
 dnp3-confirm
 dnp3-delay-measurement
 dnp3-delete-file
 dnp3-direct-operate
 dnp3-direct-operate-no-resp
 dnp3-disable-unsolicited
 dnp3-enable-unsolicited
 dnp3-freeze
 dnp3-freeze-at-time
 dnp3-freeze-at-time-no-resp
 dnp3-freeze-clear
 dnp3-freeze-clear-no-resp
 dnp3-freeze-no-resp
 dnp3-get-file-information
 dnp3-initialize-application
 dnp3-initialize-data
 dnp3-open-file
 dnp3-operate
 dnp3-read
 dnp3-record-current-time
 dnp3-save-configuration
 dnp3-select
 dnp3-start-application
 dnp3-stop-application
 dnp3-unsolicited-message
 dnp3-warm-restart
 dnp3-write

Additional function-level App-IDs can be created with the DNP3 decoder. See the next section for more details.

Table 7: DLMS

dlms-base
 dlms-get-request (functional)
 dlms-get-response (functional)
 dlms-init-req-high-level-auth (functional)
 dlms-init-req-low-level-auth (functional)
 dlms-init-req-no-auth (functional)
 dlms-init-response (functional)
 dlms-set-request (functional)
 dlms-set-response (functional)

Table 8: CN-IP

cn-ip-acknowledge
 cn-ip-base
 cn-ip-channel-membership
 cn-ip-channel-membership-req
 cn-ip-channel-routing
 cn-ip-channel-routing-req
 cn-ip-data-packet
 cn-ip-device-config-req
 cn-ip-device-configuration
 cn-ip-device-registration
 cn-ip-heartbeat-req
 cn-ip-segment
 cn-ip-send-list
 cn-ip-send-list-req

Table 9: IEC 60870-5-104

104apci-supervisory
 104apci-unnumbered
 104apci-unnumbered-startdt-act
 104apci-unnumbered-startdt-con
 104apci-unnumbered-stopdt-act
 104apci-unnumbered-stopdt-con
 104apci-unnumbered-test-act
 104apci-unnumbered-test-con
 104asdu-file-transfer
 104asdu-file-transfer-type120
 104asdu-file-transfer-type121
 104asdu-file-transfer-type122
 104asdu-file-transfer-type123

Table 9: IEC 60870-5-104 (continued)

104asdu-file-transfer-type125
 104asdu-file-transfer-type126
 104asdu-file-transfer-type127
 104asdu-param-control
 104asdu-param-control-type110
 104asdu-param-control-type111
 104asdu-param-control-type112
 104asdu-param-control-type113
 104asdu-process-control
 104asdu-process-control-type45
 104asdu-process-control-type46
 104asdu-process-control-type47
 104asdu-process-control-type48
 104asdu-process-control-type49
 104asdu-process-control-type50
 104asdu-process-control-type51
 104asdu-process-control-type58
 104asdu-process-control-type59
 104asdu-process-control-type60
 104asdu-process-control-type61
 104asdu-process-control-type62
 104asdu-process-control-type63
 104asdu-process-control-type70
 104asdu-process-monitor
 104asdu-process-monitor-type1
 104asdu-process-monitor-type10
 104asdu-process-monitor-type11
 104asdu-process-monitor-type12
 104asdu-process-monitor-type13
 104asdu-process-monitor-type14
 104asdu-process-monitor-type15
 104asdu-process-monitor-type16
 104asdu-process-monitor-type17
 104asdu-process-monitor-type18
 104asdu-process-monitor-type19
 104asdu-process-monitor-type2
 104asdu-process-monitor-type20
 104asdu-process-monitor-type21
 104asdu-process-monitor-type3

Table 9: IEC 60870-5-104 (continued)

104asdu-process-monitor-type30
 104asdu-process-monitor-type31
 104asdu-process-monitor-type32
 104asdu-process-monitor-type33
 104asdu-process-monitor-type34
 104asdu-process-monitor-type35
 104asdu-process-monitor-type36
 104asdu-process-monitor-type37
 104asdu-process-monitor-type38
 104asdu-process-monitor-type39
 104asdu-process-monitor-type4
 104asdu-process-monitor-type40
 104asdu-process-monitor-type5
 104asdu-process-monitor-type6
 104asdu-process-monitor-type7
 104asdu-process-monitor-type8
 104asdu-process-monitor-type9
 104asdu-system-control
 104asdu-system-control-type100
 104asdu-system-control-type101
 104asdu-system-control-type102
 104asdu-system-control-type103
 104asdu-system-control-type104
 104asdu-system-control-type105
 104asdu-system-control-type106
 104asdu-system-control-type107
 104asdu-system-monitor
 104asdu-system-monitor-type64
 iec-60870-5-104-base

Table 10: MMS-ICS

mms-ics-ack-event-notification
 mms-ics-additional-service
 mms-ics-alter-event-cond-monit
 mms-ics-alter-event-enroll
 mms-ics-base
 mms-ics-cancel
 mms-ics-conclude
 mms-ics-create-journal
 mms-ics-create-prog-invocations

Table 10: MMS-ICS (continued)

mms-ics-create-prog-invocation
mms-ics-define-event-action
mms-ics-define-event-condition
mms-ics-define-event-enroll
mms-ics-delete-domain
mms-ics-delete-event-action
mms-ics-delete-event-condition
mms-ics-delete-event-enroll
mms-ics-delete-journal
mms-ics-delete-prog-invocation
mms-ics-download-segment
mms-ics-eventnotification
mms-ics-file-close
mms-ics-file-delete
mms-ics-file-directory
mms-ics-file-open
mms-ics-file-read
mms-ics-file-rename
mms-ics-get-alarm-enroll-sum
mms-ics-get-alarm-summary
mms-ics-get-capability-list
mms-ics-get-domain-attribute
mms-ics-get-event-action-attr
mms-ics-get-event-cond-attr
mms-ics-get-event-enroll-attr
mms-ics-get-prog-invo-attr
mms-ics-informationreport
mms-ics-initial-download-seq
mms-ics-initialize-journal
mms-ics-initiate-upload-seq
mms-ics-kill
mms-ics-load-domain-content
mms-ics-obtain-file
mms-ics-read-journal
mms-ics-rep-event-action-stat
mms-ics-rep-event-enroll-stat
mms-ics-report-event-cond-stat
mms-ics-report-journal-status
mms-ics-report-pool-sema-stat

Table 10: MMS-ICS (continued)

mms-ics-report-sema-entry-stat
mms-ics-request-domain-download
mms-ics-request-domain-upload
mms-ics-reset
mms-ics-resume
mms-ics-start
mms-ics-stop
mms-ics-store-domain-content
mms-ics-terminate-download-seq
mms-ics-terminate-upload-seq
mms-ics-trigger-event
mms-ics-unsolicitedstatus
mms-ics-upload-segment
mms-ics-write-journal

Table 11: ICCP

iccp-base
iccp-define-named-type
iccp-define-named-variable
iccp-define-named-variable-list
iccp-define-scattered-access
iccp-define-semaphore
iccp-delete-named-type
iccp-delete-named-variable-list
iccp-write
iccp-delete-semaphore
iccp-delete-variable-access
iccp-download-segment
iccp-get-name-list
iccp-get-named-type-attr
iccp-get-scattered-access-attr
iccp-get-variable-access-attr
iccp-identity
iccp-initiate-download-seq
iccp-initiate-upload-seq
iccp-input
iccp-read
iccp-relinquish-control

Table 11: ICCP (continued)

iccp-rename
iccp-report-pool-sem-status
iccp-report-sem-entry-status
iccp-report-semaphore-status
iccp-status
iccp-take-control
iccp-terminate-download-seq
IEC-61850
IEC-61850-base
IEC-61850-delete-named-var-list
IEC-61850-getatadir

See the next section for information on how to use the **ICCP decoder** to create ICCP function-level App-IDs.

Table 12: IEEE c37.118-Synchrophasor

c37.118-cmd-frame-data-tx-off
c37.118-cmd-frame-data-tx-on
c37.118-cmd-frame-extended-frm
c37.118-cmd-frame-send-cfg-1
c37.118-cmd-frame-send-cfg-2
c37.118-cmd-frame-send-hdr-frm
c37.118-command-frame
c37.118-configuration-frame-1
c37.118-configuration-frame-2
c37.118-data-frame
c37.118-header-frame
ieee-c37.118-synchrophasor-base

Table 13: Siemens-S7

siemens-s7-base
siemens-s7-check-password-set
siemens-s7-controller
siemens-s7-download-program
siemens-s7-read
siemens-s7-set-clock
siemens-s7-setup-communication
siemens-s7-start
siemens-s7-stop
siemens-s7-upload-program
siemens-s7-warm-restart
siemens-s7-write

Table 14: Siemens S7-Comm-Plus

siemens-s7-comm-plus-base
siemens-s7-comm-plus-create-ob
siemens-s7-comm-plus-delete-ob
siemens-s7-comm-plus-download
siemens-s7-comm-plus-end-seq
siemens-s7-comm-plus-explore
siemens-s7-comm-plus-explore
siemens-s7-comm-plus-get-mtvar
siemens-s7-comm-plus-get-mtvar
siemens-s7-comm-plus-get-vsstr
siemens-s7-comm-plus-get-vsstr
siemens-s7-comm-plus-run-cpu
siemens-s7-comm-plus-set-mtvar
siemens-s7-comm-plus-set-mtvar
siemens-s7-comm-plus-set-time
siemens-s7-comm-plus-set-var
siemens-s7-comm-plus-set-var
siemens-s7-comm-plus-stop-cpu
siemens-s7-comm-plus-upload

Table 15: BACnet

bacnet-abort
bacnet-ack-alarm
bacnet-add-list-element
bacnet-atomic-read-file
bacnet-atomic-write-file
bacnet-authenticate
bacnet-base
bacnet-complex-ack
bacnet-confirmed-cov-notify
bacnet-confirmed-event-notify
bacnet-confirmed-private-xfer
bacnet-confirmed-text-message
bacnet-create-object
bacnet-delete-object
bacnet-device-comm-control

Table 15: BACnet (continued)

bacnet-error
 bacnet-error-ack-alarm
 bacnet-error-add-list-element
 bacnet-error-atomic-read-file
 bacnet-error-atomic-write-file
 bacnet-error-conf-cov-notify
 bacnet-error-conf-event-notif
 bacnet-error-conf-private-trf
 bacnet-error-conf-text-mssg
 bacnet-error-delete-object
 bacnet-error-device-comm-cntrl
 bacnet-error-get-alarm-summary
 bacnet-error-get-enrollment-sum
 bacnet-error-get-event-info
 bacnet-error-life-safety-oper
 bacnet-error-read-property
 bacnet-error-read-property-cond
 bacnet-error-read-property-mul
 bacnet-error-read-range
 bacnet-error-reinitialize-dev
 bacnet-error-remove-list-elem
 bacnet-error-request-key
 bacnet-error-subscribe-cov
 bacnet-error-subscribe-cov-prop
 bacnet-error-vt-data
 bacnet-error-vt-open
 bacnet-error-write-prop-mult
 bacnet-get-alarm-summary
 bacnet-get-enrollment-summary
 bacnet-get-event-information
 bacnet-i-am
 bacnet-i-have
 bacnet-life-safety-operation

Table 15: BACnet (continued)

bacnet-read-prop-conditional
 bacnet-read-prop-multiple
 bacnet-read-property
 bacnet-read-range
 bacnet-reinitialize-device
 bacnet-reject
 bacnet-remove-list-element
 bacnet-request-key
 bacnet-segment-ack
 bacnet-simple-ack
 bacnet-subscribe-cov
 bacnet-subscribe-cov-property
 bacnet-time-synchronization
 bacnet-unconfirmed-cov-notif
 bacnet-unconfirmed-event-notif
 bacnet-unconfirmed-private-txfr
 bacnet-unconfirmed-text-message
 bacnet-utc-time-synchronization
 bacnet-vt-close
 bacnet-vt-data
 bacnet-vt-open
 bacnet-who-has
 bacnet-who-has-access-credent
 bacnet-who-has-access-door
 bacnet-who-has-access-point
 bacnet-who-has-access-right
 bacnet-who-has-access-user
 bacnet-who-has-access-zone
 bacnet-who-has-accumulator
 bacnet-who-has-analog-input
 bacnet-who-has-analog-output
 bacnet-who-has-analog-value
 bacnet-who-has-averaging
 bacnet-who-has-binary-input

Table 15: BACnet (continued)

bacnet-who-has-binary-output
bacnet-who-has-binary-value
bacnet-who-has-bitstring-value
bacnet-who-has-calendar
bacnet-who-has-command
bacnet-who-has-cred-data-input
bacnet-who-has-date-pattern-val
bacnet-who-has-date-value
bacnet-who-has-device
bacnet-who-has-event-enrollment
bacnet-who-has-event-log
bacnet-who-has-global-group
bacnet-who-has-group
bacnet-who-has-integer-value
bacnet-who-has-large-analog-val
bacnet-who-has-life-safety-pt
bacnet-who-has-life-safety-zone
bacnet-who-has-multi-state-in
bacnet-who-has-multi-state-out
bacnet-who-has-multi-state-val
bacnet-who-has-network-security
bacnet-who-has-notification-cls
bacnet-who-has-octatestring-val
bacnet-who-has-pulse-converter
bacnet-who-has-schedule
bacnet-who-has-structured-view
bacnet-who-has-time-pattern-val
bacnet-who-has-time-value
bacnet-who-has-trend-log
bacnet-who-has-trend-log-mul
bacnet-who-is
bacnet-write-prop-multiple
bacnet-write-property
bacnet-who-has-time-value
bacnet-who-has-trend-log-mul

Table 16: ADDP

addp-base
addp-dhcp-network-config-req (functional)
addp-dhcp-network-config-resp (functional)
addp-discovery-request (functional)
addp-discovery-response (functional)
addp-reboot-request (functional)
addp-reboot-response (functional)
addp-static-network-config-req (functional)
addp-static-network-config-resp (functional)

Table 17: KNXNET

knxnet-ip-base
knxnet-ip-configuration-request (functional)
knxnet-ip-connect-request (functional)
knxnet-ip-connection-state-req (functional)
knxnet-ip-description-request (functional)
knxnet-ip-disconnect-request (functional)
knxnet-ip-search-request (functional)
knxnet-ip-tunnelling-request (functional)

Table 18: COAP

coap-base
coap-delete-request (functional)
coap-get-request (functional)
coap-post-request (functional)
coap-put-request (functional)

Table 19: OPC-UA

opc-ua-acknowledge (functional)
opc-ua-activate-session-req (functional)
opc-ua-add-nodes-req (functional)
opc-ua-add-references-req (functional)
opc-ua-browse-next-req (functional)
opc-ua-browse-req (functional)
opc-ua-call-method-req (functional)
opc-ua-call-req (functional)
opc-ua-cancel-req (functional)
opc-ua-close (functional)
opc-ua-close-secure-channel-req (functional)
opc-ua-close-session-req (functional)
opc-ua-create-session-req (functional)
opc-ua-create-subscription-req (functional)
opc-ua-delete-nodes-req (functional)
opc-ua-delete-references-req (functional)
opc-ua-delete-subscriptions-req (functional)
opc-ua-error (functional)
opc-ua-find-server-req (functional)
opc-ua-get-endpoints-req (functional)
opc-ua-hello (functional)
opc-ua-history-read-req (functional)
opc-ua-history-update-req (functional)
opc-ua-open (functional)
opc-ua-open-secure-channel-req (functional)
opc-ua-publish-req (functional)
opc-ua-query-first-req (functional)

Table 19: OPC-UA (continued)

opc-ua-query-next-req (functional)
 opc-ua-read-req (functional)
 opc-ua-register-nodes-req (functional)
 opc-ua-register-servers-req (functional)
 opc-ua-republish-req (functional)
 opc-ua-set-monitoring-mode-req (functional)
 opc-ua-set-publishing-mode-req (functional)
 opc-ua-set-triggering-req (functional)
 opc-ua-unregister-node-req (functional)
 opc-ua-write-req (functional)

Table 20: GPRS

gtp-base
 gtp-prime
 gtp-u
 gtpv0
 gtpv1-c
 gtpv2-c

Table 21: SS7

ss7-map-ggsn-callingparty
 ss7-map-siwf-callingparty
 ss7-mapsgsn-callingparty
 ss7-map-hlr-callingparty
 ss7-map-vlr-callingparty
 ss7-map-msc-callingparty
 ss7-map-eir-callingparty
 ss7-map-gsmf-callingparty
 ss7-map-gmlc-callingparty
 ss7-map-siwf-callingparty
 ss7-map-sgsn-callingparty
 ss7-map-ggsn-callingparty
 ss7-map-css-callingparty

Table 22: Ethercat

ethercat-base
 ethercat-device-protocol
 ethercat-mailbox-data
 ethercat-process-data

Table 23: GE-srtp

ge-srtp-base
 ge-srtp-change-cpu-privilege (functional)
 ge-srtp-change-cpu-privilege (functional)
 ge-srtp-get-control-program (functional)
 ge-srtp-get-controller-info (functional)
 ge-srtp-get-fault-table (functional)
 ge-srtp-get-plc-time (functional)
 ge-srtp-plc-short-status-req (functional)
 ge-srtp-program-load (functional)
 ge-srtp-program-store (functional)

Table 23: GE-srtp (continued)

ge-srtp-programmer-logon (functional)
 ge-srtp-read-program-mem (functional)
 ge-srtp-read-sys-mem (functional)
 ge-srtp-read-task-mem (functional)
 ge-srtp-set-control-id (functional)
 ge-srtp-set-plc (functional)
 ge-srtp-set-plc-time (functional)
 ge-srtp-toggle-force-sys-mem (functional)
 ge-srtp-write-program-blk-mem (functional)
 ge-srtp-write-sys-mem (functional)
 ge-srtp-write-task-mem (functional)

Table 24: Tristation

tristation-base
 tristation-connect-req (functional)
 tristation-connect-rsp (functional)
 tristation-disconnect-req (functional)
 tristation-get-cp-status-req (functional)
 tristation-get-cp-status-rsp (functional)
 tristation-run-program (functional)

Table 25: Schneider

umas
 umas-base
 umas-init-comm
 umas-plc-reservation-take
 umas-plc-reservation-release
 umas-memory-block-read
 umas-memory-block-write
 umas-variables-read
 umas-variables-write
 umas-coils-registers-read
 umas-coils-registers-write
 umas-initialize-upload
 umas-upload-block
 umas-initialize-download
 umas-download-block
 umas-sd-backup-make
 umas-sd-backup-restore
 umas-sd-backup-remove
 umas-plc-start
 umas-plc-stop
 umas-repeat-request
 umas-monitor-bits-read
 umas-monitor-bits-write
 umas-monitor-words-read
 umas-monitor-words-write
 umas-io-object-write
 umas-read-id

Custom App-ID Decoders

Protocol decoders are also provided in PAN-OS to allow creation of custom App-IDs. For more information on the use of application protocol decoders to create custom App-IDs, refer to the [PAN-OS Administrator's Guide section on custom applications](#).

For ICS protocols, both a DNP3 decoder and ICCP decoder are available.

DNP3 Decoder

The DNP3 protocol standard defines 33 function codes: 31 request functions and two response functions. The DNP3 protocol decoder included in PAN-OS exposes the Function Code field as a “context” such that users can specify for which function code variant of the DNP3 protocol they would like to create a custom App-ID.

The DNP3 decoder also exposes the Object Type field as another context to users. This allows for the creation of custom App-IDs with varying Object Types. The function code context and the object type can be logically ANDed to create a unique function-code and object-type combination.

ICCP Decoder

Similarly, the ICCP protocol decoder included in PAN-OS exposes the Function Code field as a “context” such that users can specify for which function code variant of the ICCP protocol they would like to create a custom App-ID.

IEC104 Decoder

The IEC-60870-5-104 protocol standard defines 68 function codes. The IEC 104 decoder included in PAN-OS exposes the Function Code field as a “context,” allowing users to specify the function code variant of IEC-60870-5-104 for which they would like to define a custom App-ID.

Submitting New App-ID Requests

If your App-ID of interest is not available in Applipedia, you can submit new App-ID requests for review at: <http://researchcenter.paloaltonetworks.com/submit-an-application>.

In addition to your online request, please provide your Palo Alto Networks systems engineer with the following information, along with your new App-ID requests:

1. **Reference packet captures (PCAPs) for the application/traffic of interest.** Make sure to include full session setup and close for each type of traffic of interest. These are the most important items used by our engineers in creating new App-IDs. To facilitate analysis, multiple PCAPs of short sessions, each covering one protocol and a particular traffic type of interest, are preferred over long session PCAPs covering multiple protocols and function types.
2. **Description of the traffic flow, IP address, and associated devices.** This background is helpful for our engineering team developing the App-IDs.
3. **Documentation of the ICS protocol or application.** More detailed protocol/application documentation is better, especially documents that describe the ports used and the packet structure.
4. **Technical contact person from the requester and/or ICS vendor.** Engineering often needs to interact with the requester to get more technical information or additional PCAP specimens to help in developing a robust App-ID. Having a fixed technical point of contact facilitates faster turnaround time. It would also be beneficial to have a contact point at the actual ICS vendor who has deep expertise on the protocol of interest.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_ds_app-ids-ics-scada_080822