Cisco ISA 3000 Industrial Protocol Support

Overview

This document lists the industrial protocols the Cisco Industrial Security Appliance ISA 3000 can inspect as of December 2020. Industrial protocols are supported for 2 use cases:

- Application detection
- Command and payload detection

Application detection

Application detectors (AppID) are used to detect **protocols** or an **application transactions** in the traffic passing through the firewall. The following ICS/OT AppIDs are supported by ISA 3000 Firepower software.

OT Application Detectors		
• BACNet	• COSEM	• Fujitsu Device Control
• Modbus	• GOOSE	• Emission Control Protocol
• DNP3	• GSE	• Honeywell Control Station/NIF Server
• IEC 60870-5-104	• OPC-UA	• Honeywell Experion DSA Server Monitor
• Ethernet/IP (ENIP)	• TPKT	• OMRON FINS
• ISO MMS	• COTP	• Q.931
• CIP (Common Industrial Protocol)	• CIP Admin • CIP Infrastructure • CIP Malformed • CIP Read • CIP Write • CIP Unknown • CIP RA Admin Download • CIP RA Firmware Update • CIP RA Admin Other • CIP RA Infrastructure • CIP RA Read Other • CIP RA Read Tag • CIP RA Write Other • CIP RA Write Tag	

Command and payload detection in OT traffic

Deep packet inspection (DPI) is performed to detect commands and payload in the OT application traffic. The following protocols are supported by ISA 3000 Firepower software.

OT Command and Payload Detection
Modbus
DNP3
CIP (Common Industrial Protocol)
IEC 60870-5-104
IEC 61850 MMS

Modbus

Function/Command	Payload Inspection options
• read_coils • read_discrete_inputs • read_holding_registers • read_input_registers • write_single_coil • write_single_register • read_exception_status • diagnostics • get_comm_event_counter • get_comm_event_log • write_multiple_coils • write_multiple_registers • report_slave_id • read_file_record • write_file_record • mask_write_register • read_write_multiple_registers • read_fifo_queue • encapsulated_interface_transport	• Modbus Unit (address of PLC) • Modbus Data

DNP3

Function/Command	Payload options

• confirm
• read
• write
• select
• operate
• direct_operate
• direct_operate_nr
• immed_freeze
	• DNP3 Data
	• DNP3 Object Headers
	• DNP3 Internal Indicator Flags
	  • all_stations
	  • class_1_events
	  • class_2_events
	  • class_3_events
	  • need_time

• immed_freeze_nr • freeze_clear • freeze_clear_nr • freeze_at_time • freeze_at_time_nr • cold_restart • warm_restart • initialize_data • initialize_appl • start_appl • stop_appl • save_config • enable_unsolicited • disable_unsolicited • assign_class • delay_measure • record_current_time • open_file • close_file • delete_file • get_file_info • authenticate_file • abort_file • activate_config • authenticate_req • authenticate_err • response • unsolicited_response • authenticate_resp	• local_control • device_trouble • device_restart • no_func_code_support • object_unknown • parameter_error • event_buffer_overflow • already_executing • config_corrupt • reserved_2 • reserved_1

CIP

Following CIP options are supported, combination of below options enables detection of 100's of CIP functions and commands

CIP Options
• CIP Attribute • CIP Class • CIP Connection Path Class • CIP Instance • CIP Request • CIP response • CIP Service Code • CIP Status

IEC 61850 MMS

Function/Command
• MMS Confirmed-RequestPDU • MMS Confirmed-ResponsePDU

- MMS Confirmed-ErrorPDU
- MMS UnconfirmedPDU
- MMS RejectPDU
- MMS Cancel-RequestPDU
- MMS Cancel-ResponsePDU
- MMS Cancel-ErrorPDU
- MMS Initiate-RequestPDU
- MMS Initiate-ResponsePDU
- MMS Initiate-ErrorPDU
- MMS Conclude-RequestPDU
- MMS Conclude-ResponsePDU
- MMS Conclude-ErrorPDU
- MMS Confirmed-RequestPDU status message
- MMS Confirmed-RequestPDU identify message
- MMS Confirmed-RequestPDU rename message
- MMS Confirmed-RequestPDU getNameList message
- MMS Confirmed-RequestPDU read message
- MMS Confirmed-RequestPDU write message
- MMS Confirmed-RequestPDU defineScatteredAccess message
- MMS Confirmed-RequestPDU defineNamedVariableList message
- MMS Confirmed-RequestPDU getVariableAccessAttributes message
- MMS Confirmed-RequestPDU defineNamedVariable message
- MMS Confirmed-RequestPDU deleteVariableAccess message
- MMS Confirmed-RequestPDU getScatteredAccessAttributes message
- MMS Confirmed-RequestPDU getNamedVariableListAttributes message
- MMS Confirmed-RequestPDU deleteNamedVariableList message
- MMS Confirmed-RequestPDU defineNamedType message
- MMS Confirmed-RequestPDU getNamedTypeAttributes message
- MMS Confirmed-RequestPDU deleteNamedType message
- MMS Confirmed-RequestPDU input message
- MMS Confirmed-RequestPDU output message
- MMS Confirmed-RequestPDU takeControl message
- MMS Confirmed-RequestPDU relinquishControl message
- MMS Confirmed-RequestPDU defineSemaphore message
- MMS Confirmed-RequestPDU deleteSemaphore message
- MMS Confirmed-RequestPDU reportSemaphoreStatus message
- MMS Confirmed-RequestPDU reportPoolSemaphoreStatus message
- MMS Confirmed-RequestPDU reportSemaphoreEntryStatus message
- MMS Confirmed-RequestPDU initiateDownloadSequence message
- MMS Confirmed-RequestPDU downloadSegment message
- MMS Confirmed-RequestPDU terminateDownloadSequence message
- MMS Confirmed-RequestPDU initiateUploadSequence message
- MMS Confirmed-RequestPDU uploadSegment message
- MMS Confirmed-RequestPDU terminateUploadSequence message
- MMS Confirmed-RequestPDU DomainDownload message
- MMS Confirmed-RequestPDU loadDomainContent message
- MMS Confirmed-RequestPDU storeDomainContent message
- MMS Confirmed-RequestPDU DomainUpload message
- MMS Confirmed-RequestPDU getDomainAttributes message
- MMS Confirmed-RequestPDU deleteProgramInvocation message
- MMS Confirmed-RequestPDU createProgramInvocation message

- MMS Confirmed-RequestPDU deleteDomain message
- MMS Confirmed-RequestPDU stop message
- MMS Confirmed-RequestPDU start message
- MMS Confirmed-RequestPDU resume message
- MMS Confirmed-RequestPDU reset message
- MMS Confirmed-RequestPDU kill message
- MMS Confirmed-RequestPDU getProgramInvocationAttributes message
- MMS Confirmed-RequestPDU obtainFile message
- MMS Confirmed-RequestPDU defineEventCondition message
- MMS Confirmed-RequestPDU triggerEvent message
- MMS Confirmed-RequestPDU alterEventConditionMonitoring message
- MMS Confirmed-RequestPDU getEventConditionAttributes message
- MMS Confirmed-RequestPDU reportEventConditionStatus message
- MMS Confirmed-RequestPDU deleteEventAction message
- MMS Confirmed-RequestPDU deleteEventCondition message
- MMS Confirmed-RequestPDU defineEventAction message
- MMS Confirmed-RequestPDU reportEventActionStatus message
- MMS Confirmed-RequestPDU getEventActionAttributes message
- MMS Confirmed-RequestPDU defineEventEnrollment message
- MMS Confirmed-RequestPDU reportEventEnrollmentStatus message
- MMS Confirmed-RequestPDU deleteEventEnrollment message
- MMS Confirmed-RequestPDU getEventEnrollmentAttributes message
- MMS Confirmed-RequestPDU alterEventEnrollment message
- MMS Confirmed-RequestPDU acknowledgeEventNotification message
- MMS Confirmed-RequestPDU getAlarmSummary message
- MMS Confirmed-RequestPDU getAlarmEnrollmentSummary message
- MMS Confirmed-RequestPDU readJournal message
- MMS Confirmed-RequestPDU writeJournal message
- MMS Confirmed-RequestPDU initializeJournal message
- MMS Confirmed-RequestPDU reportJournalStatus message
- MMS Confirmed-RequestPDU deleteJournal message
- MMS Confirmed-RequestPDU getCapabilityList message
- MMS Confirmed-RequestPDU createJournal message
- MMS Confirmed-RequestPDU fileClose message
- MMS Confirmed-RequestPDU fileOpen message
- MMS Confirmed-RequestPDU fileRename message
- MMS Confirmed-RequestPDU fileDirectory message
- MMS Confirmed-RequestPDU fileDelete message
- MMS Confirmed-RequestPDU fileRead message
- MMS Confirmed-RequestPDU informationReport message

IEC 60870-5-104 (IEC-104)

Function/Command	
• IEC 104 STARTDT ACT	• IEC 104 M_SP_TB_1
• IEC 104 STARTDT CON	• IEC 104 M_IT_NA_1
• IEC 104 STOPDT ACT	• IEC 104 M_ST_TB_1
• IEC 104 STOPDT CON	• IEC 104 M_ME_TD_1
• IEC 104 TESTFR ACT	• IEC 104 M_BO_TB_1
• IEC 104 TESTFR CON	• IEC 104 M_ME_TE_1
• IEC 104 Ack file	• IEC 104 M_ME_TF_1

- IEC 104 Double point information
- IEC 104 End of initialization
- IEC 104 File ready
- IEC 104 Integrated totals
- IEC 104 Interrogation command
- IEC 104 Last section
- IEC 104 List directory
- IEC 104 Measured value
- IEC 104 Packed start events
- IEC 104 Parameter value
- IEC 104 Query Log
- IEC 104 Read command
- IEC 104 Regulating step command
- IEC 104 Rest process command
- IEC 104 Set point command
- IEC 104 Single command
- IEC 104 Single point information
- IEC 104 Step point information
- IEC 104 Test command with time tag
- IEC 104 bitstring of 32 bits
- IEC 104 clock sync command
- IEC 104 counter interrogation command
- IEC 104 double command issued
- IEC 104 unknown ASDU type detected
- IEC 104 traffic to/from EXTERNAL_NET
- IEC 104 traffic to/from EXTERNAL_NET
- IEC 104 force off denial of service attempt
- IEC 104 force on denial of service attempt
- IEC 104 M_SP_NA_1
- IEC 104 M_DP_NA_1
- IEC 104 M_ST_NA_1
- IEC 104 M_BO_NA_1
- IEC 104 M_ME_NA_1
- IEC 104 M_ME_NB_1
- IEC 104 M_ME_ND_1
- IEC 104 M_DP_TB_1
- IEC 104 M_ME_NC_1
- IEC 104 M_PS_NA_1
- IEC 104 M_IT_TB_1
- IEC 104 M_EP_TD_1
- IEC 104 M_EP_TE_1
- IEC 104 M_EP_TF_1
- IEC 104 C_SC_NA_1
- IEC 104 C_DC_NA_1
- IEC 104 C_RC_NA_1
- IEC 104 C_SE_NA_1
- IEC 104 C_SE_NB_1
- IEC 104 C_SE_NC_1
- IEC 104 C_BO_NA_1
- IEC 104 C_SC_TA_1
- IEC 104 C_DC_TA_1
- IEC 104 C_RC_TA_1
- IEC 104 C_SE_TA_1
- IEC 104 C_SE_TB_1
- IEC 104 C_SE_TC_1
- IEC 104 C_BO_TA_1
- IEC 104 M_EI_NA_1
- IEC 104 C_TS_TA_1
- IEC 104 P_ME_NA_1
- IEC 104 P_ME_NB_1
- IEC 104 C_CI_NA_1
- IEC 104 C_RD_NA_1
- IEC 104 C_IC_NA_1
- IEC 104 C_CS_NA_1
- IEC 104 C_RP_NA_1
- IEC 104 P_ME_NC_1
- IEC 104 F_AF_NA_1
- IEC 104 F_FR_NA_1
- IEC 104 P_AC_NA_1
- IEC 104 F_SR_NA_1
- IEC 104 F_SC_NA_1
- IEC 104 F_LS_NA_1
- IEC 104 F_SG_NA_1
- IEC 104 F_DR_TA_1
- IEC 104 F_SC_NB_1

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

12/2020