

持续威胁检测 (CTD) 支持的协议

CTD 5.1.1 版本 | Edge 3.6 版本

2025 年 4 月

www.claroty.com | ©2025 Claroty Ltd. All rights reserved

目录

引言	3
被动协议 (Passive Protocols)	4
主动查询 (Active Queries)	10
项目文件 (Project Files)	14
Edge 3.6 版本支持 Windows 7 广播查询	16
Edge 3.6 版本支持 Windows 7 单播查询	17
Edge 3.6 版本支持项目文件 (Project Files)	21

引言

持续威胁检测 (CTD) 支持业界最全面的工业协议，涵盖了运营技术 (OT)、物联网 (IoT)、工业物联网 (IIoT)、楼宇管理系统 (BMS) 以及信息技术 (IT) 领域的标准和专有协议。

这得益于Claroty的跨学科研究团队，该团队与行业领先的工业制造商、供应商、利益相关方紧密合作，可确保Claroty的产品支持最多的工业协议，保持工业网络安全研究实验室的领先地位，还继续支持Claroty的客户与社区最需要的协议、研究和产品。

被动协议 (Passive Protocols)

Standard

- ARP
- BACNET
- CAPWAP
- Citect HMI
- Cotp
- DHCP
- Digi real port
- DLMS COSEM
- DNP3
- E-Terra Workstation
- Ethernet POWERLINK
- ETHERNET/IP
- FactoryTalk RNA
- Foundation Fieldbus (FF)
- HART-IP
- Hot Standby Router Protocol (HSRP)
- HTTP
- HTTP-XML (specific schemes)
- IEC101
- IEC103
- IEC104
- IMAP
- ITEPM - Endpoint Mapper
- LLDP
- MDLC Proprietary
- MMS (IEC-61850/ICCP/TASE.2)
- Modbus
- Modbus Execload
- Modbus Xinje
- MQTT
- DeltaV
- Ovation
- Ovation ADMD
- Ovation Alarm
- NetBIOS Browser (UDP 138)
- NetBIOS Datagram Service
- NTP
- OPC-DA
- OPC-UA
- POP3
- Profinet DCP
- Profinet I/O
- Profinet Real-Time
- Prosoft Discovery
- PRP
- PTP
- Radius
- RTCP
- Sattbus
- SECSGEM
- SIP
- SNMP

- SSH
- Synchrophasor
- TFTP
- TTSAC (Sistema Avanzado de Control)
- VNC
- X-Pact Data

ABB

- Bailey
- DMS system
- HC800 (Infinet)
- MasterBus 300
- Melody
- Net Config
- RNRP
- Spirit
- Symphony Plus
- Totalflow

Alien RFID

- Alien RFID Reader Heartbeat

Alstom

- Alsipa (Multicast messages)

- E-Terra

Atlas

- Atlas ALnet

AVIVA (Schneider)

- ClearSCADA ViewX

B&R

- B&R INA2000

Beckhoff

- AMS (ADS)
- EtherCAT

Bristol

- BSAP

Buffalo

- NASNavigator

Caterpillar

- Caterpillar AHS

CC Link

- SLMP (CC Link IE Field Basic)

CC Link IE

- CC Link IE - Field

Checkpoint

- CPHA (Checkpoint High Availability)

Cisco

- Discovery Protocol (CDP)
- Skinny (SCCP)
- UDLD

CODESYS

- CodesysV2
- CodesysV3

Cognex

- Cognex Discovery

Control

- Control NS Link

Control Technologies Inc.

- Control Technologies Inc. (CTI)

Cygnnet

- Cygnnet SCADA

Dropbox

- Dropbox LAN-sync

Eltec

- Modbus Eltec

Emerson

- DeltaV
- Ovation
- Ovation ADMD
- Ovation Alarm
- Ovation DBXmit
- Ovation PTEdit
- OvationRPC
- ROC Plus
- Telnet - DeltaV

Enedis

- B32

Foxboro

- Foxboro LLC
- Foxboro RTV

Fuji Electric

- FI-net fuji

Fanuc

Fanuc Discovery

GE

- GE Bentley Nevada (BNC3500)
- GE PAC8000 (AXE)
- GE QuickPanel (TRAPI+HTTP)
- GE SDI (MarkVie)
- GE SDI Classic (MarkVie)
- GE SRTIP
- GE-ALM
- GE-EGD
- GE-EGD-CMP
- GE-iFix
- Modbus GE Enervista

Hikvision

- Hikvision Discovery Protocols

Hirschmann

- HiDiscovery
- Telnet - Hirschmann

Honeywell

- Honeywell C200 - Ftebcip
- Honeywell EpicMo (C300 management)
- Honeywell Experion - CeeNTComm (C300,EHPM)
- Honeywell Firewall CF9

HP

- HP Switch

IEC

- Goose (IEC-61850)

jema

- FL-net - All

Keyence

- Keyence Host-Link Communication
- Keyence KV Studio
- Keyence Logger

Knapp

- Knapp

KNXnet

- IP

Kongsberg

- Kongsberg

Koyo

- Koyo (HEI/K-Sequence/DirectNet)

Lantronix

- Lantronix Serial GW

Linux

- Linux High Availability

LS Electric

- XG5000 Discovery
- RAPIEnet

Matrikon

- Matrikon OPC Tunneller

Meggitt

- Vibro-Meter

Microsoft

- CIFS (SMB)
- DCE RPC
- DCE RPC - ABB DCS Service Manager
- Microsoft RDP
- NTLMSSP (Auth protocol)
- SAMR
- TDS
- Windows Update Delivery Optimization

Mikrotik

- MNDP

Mitsubishi

- Melsec
- Melsec

Motorola

- MDLC data
- MDLC management
- MDLC proprietary

Moxa

- Telnet - Moxa

Niagara

- Tridium

NMEA

- NMEA-0183

Nortel

- NDP

OCPP

- OCPP 1.6

Omniflow

- Omniflow Flow computer
- Telnet - Omniflow

Omron

- FINS

Opto

- OPTO
- OPTO MMP
- OPTO SoftPAC Agent

OSISoft

- PI1

- PI3

Pepperl+Fuchs

- P+F DCP

Pheonix Contact

- ProConoS (TCP 20547)

Plum

- Gaz Modem

Portwell

- Portwell

Red Lion

- Red lion Crimson
- Red Lion NView-2 Discovery

Rockwell

- CIP
- DPI (over PCCC)
- ENIP
- PCCC

Ruggedcomm

- RCDP

SAIAS

- SBUS

ScadaPack

- Modbus ScadaPack

Schneider

- Modbus Modsoft
- Modbus Schneider
- PowerLogic Discovery
- Schneider NetManage
- Schneider EGX UDP 59
- Schneider ION
- Triconex Tristation
- Triconex TSAA

Schweitzer

- FTP - SEL
- Telnet - SEL

SICK

- CoLa-A

Siemens

- Cargo Compact

- Cargo Compact Sensor
- Cargo Compact Control
- Digs4 (Siprotec 4)
- Digs5
- P2
- S7Comm
- S7Comm Plus
- Siemens FWL LOAD (firmware upload)
- Siemens IEM
- Sinaut FW8
- T3000 Protocols

SMA

- Sunny WEBBOX

Smiths

- Detection Broadcast

SMS Group

- X-Pact Diagnostics
- X-Pact Discovery

Spotify

- Spotify P2P

TC

- Net

TCNOpen

- TRDP Process Data

Televent

- OASyS

Terasaki

- Negotiation
- Realtime Data Sync

Themis

- Enhanced Modbus

Toshiba

- Net1G

Toyoda

- PCWin

Toyota

- FI-net Toyoda

Trend

- IQ3
- WAGO

TwinSoft

- Modbus Twinsoft

Valmet

- MaxDNA (maxNET)
- Valmet DNA Alarms
- Valmet DNA Damatic configuration, data

- Valmet DNA Data
- Valmet DNA Frontend

Willowglen

- DACP

Wonderware

- Wonderware SuiteLink

- IOTalk

Yokogawa

- ODEQ
- VNET (VHF)

主动查询 (Active Queries)

Standard

- BACnet Discovery
- BACnet Query
- DB Enumeration Query (mssql, mysql, mongo)
- DNP3
- EN/IP Query
- EN/IP Scan
- Exi 3000 Query
- Exi 3000 Discovery
- FTP Query
- HTTP Query
- IoT Query
- mDNS Query
- mDNS Discovery
- Modbus Information Object
- MMS Query
- NetBIOS
- PCCC Query
- Ping Sweep
- Profinet-DCP Query
- Profinet-DCP Scan
- Reverse DNS
- SNMP Network Layout Query
- SNMP Query
- SNMP Scan
- SNMP Siprotec 5

- SSDP
- SSH Discovery
- SSH Query
- TCP Port Discovery
- TCP Port Scan
- Telnet
- WSD Discovery

ABB

- Bacnet

Anord Mardix

- HTTP

Atlas Copco

- Atlas Copco ToolsTalk Query
- Atlas Copco MWR HTTP Query
- Atlas Copco WebSocket Query

Automation Direct

- C-more HMI Discovery
- C-more HMI Unicast

AutomatedLogic

- Bacnet

Banner Engineering

- Banner Engineering DXM Query

Brightwell

- DBTalk Query

B&R

- B&R HTTP
- B&R Profile
- B&R Query

Beckhoff

- Beckhoff Query

Carel

- Bacnet

CIP

- CIP Query

CODESYS

- CodesysV3 Discovery

Cisco

- Cisco Profile
- CTI Query

Cognex

- Cognex Query

CrowdStrike

- CrowdStrike Discovery
- CrowdStrike Query

GE

- GE-SRTP
- GE Station Manager Query

Ex-i

- Exi3000 Discovery
- Exi3000 Query

Hikvision

- Hikvision SADP Query

- Hikvision SADP Discovery

Fanuc

- Focas Query

Festo

- Festo Broadcast Discovery

Hirschmann

- Hirschmann Discovery Query
- Hirschmann Discovery Scan

Indraworks

- Indraworks Discovery
- Indraworks Query

Janitza

- SNMP
- HTTP
- Janitza Query

Koyo

- Koyo Directlogic query

Lantronix

- Hirschmann Profile

- Unicast Query

- Broadcast Discovery

LS

- LS Discovery

LS Electric

- LS Electric XG5000 Query

Microsoft

- MS SQL
- Windows Profile
- WinRM Query
- WMI Query
- WSD Discovery
- WSD Query

Mitsubishi

- Beijer HMI Query
- Melsoft Discovery
- Melsoft Query
- Mitsubishi Profile
- Mitsubishi GOT Discovery
- Mitsubishi GOT Query

Moxa

- Broadcast Scan

- Unicast Scan

Niagara

- Tridium Fox Query

Omron

- FINS Discovery
- FINS Query
- PLC Query
- Omron Modbus Query

Opto22

- Opto22 Query

Ovarro

- TBox Query

Pepperl+-Fuchs

- DCP Query

RAFT

- Gateway Scan
- Gateway Query

Red Lion

- Sixtnet Query

Rockwell

- CIP Query
- PCCC
- Rockwell Profile

Schneider Electric

- Modicon Discovery
- SCADAPack ES DNP3 query
- Schneider ION
- Schneider SmartX
- Schneider TSX Query
- Schneider Unity Query

SensoPart

- SensoPart VISOR Discovery

Siemens

- CTI Query
- S7Comm Query
- S7CommPlus Query
- Siemens Profile
- Siprotec 5 Profile

Sinumeric

- Sinumeric Query

Sixnet

- Sixnet Discovery
- Sixnet Query

SMA

- Speedwire Discovery Query
- Speedwire Discovery

Toyoda

- PCWin Query

Tridium

- Fox Query

Ubiquiti

- Ubiquiti Query

Unitronics

- Unitronics Query

Vamp

- Modbus

VMware

- VMware ESX Discovery

WAGO

- WAGO Query

Westermo

- WeConfig

Zebra

- Zebra Printer Discovery

项目文件 (Project Files)

Standard

- SCL

ABB

- 800xA
- AC800M
- Advant
- Composer
- RTU5XX SCADA Vantage
- Totalflow PCCU

Beckhoff

- TwinCAT3

B&R

- Automation Studio v3/v4

CODESYS

- CodesysV3

Emmerson

- DeltaV

FANUC

- ZIP Files

Fuji

- SX-Programmer (D300Win)

GE

- Bently Nevada
3500 System Configuration
- MarkVI ToolBoxST
- rx3i,9030 Proficy Machine
- rx3i,9030 PacsAnalyzer

Honeywell

- EHPM
- Experion Ctools / SIT

Kuka

- Robots

Kepware

- Kepware OPC

LS

- XG5000

Mitsubishi

- GX Works2

- GX Works3
- Melsec GX Developer
- DIASYS Netmation

Motorola

- ACE, MOSCAD ACE3600

Omron

- CX-One
- Sysmac Studio

Red Lion

- Red Lion HMIs Crimson
v3.0/3.1

Rockwell

- AAdvance Log Collection
- AssetCentre
- FactoryTalkView / RSVIEW
- ICSTriplex Log Collection
- ISaGRAF (multiple)
- MicroLogix Factory View
- MicroLogix RS System
Ferret
- RSLogix 5000 / 500 / 5

- RSLinx
- Trusted TMR IEC 1131 Toolset

Schneider

- Concept
- EcoStruxure Building Ops
- M221 SoMachine
- Modicon/Quantum
- SCADAPack 32 Telespace Studio
- TSX Micro, Premium PL7
- TwidoSuite
- GP-3000 GP-Pro EX
- GP-4000 GP-Pro EX
- LT-3000 GP-Pro EX
- LT-4000 GP-Pro EX
- IPC (PC/AT)
- SP-5000 GP-Pro EX

- ST-3000 IPC (PC/AT) GP-Pro EX

SEL

- AcSELerator
- AcSELerator QuickSet
- AcSELerator RTAC

SICK

- Sopas ET

Siemens

- LOGO!Soft Comfort
- PCS7
- Proneta
- S7 TiaPortal (v13/v14/v15/v16/v17/v18,v19)

- S7/T3000 Step7
- Simatic Softshop 505
- Siprotec Digi4 / Digi5
- TIA Portal Project Server
- TIA Portal V18 & 19

Toyoda

- PCWin

Triconex

- Tricon/Trident/TriGP
- TriStation 1131

Xinje

- Xinje PLCs XDPPro

Yokogawa

- Centum VP/CS3000
- ProsafeRS

Edge 3.6 版本支持 Windows 7 广播查询

Standard

- BACNET
- EN/IP
- ICMP Broadcast
- MDNS
- SSDP
- Profinet DCP
- WSD

Bosh

- Indraworks Discovery

Codesys/ Standard

- Codesys Discovery

Exi

- Exi3000 Discovery

GE

- GE Station Manager Discovery

Hirschman

- HiDiscovery

- SNMP
- HTTP

Lantronix

- Lantronix Broadcast Discovery

LS

- XG5000 Discovery

Mitsubishi

- Melsoft Discovery
- Mitsubishi GOT Discovery

Moxa

- Moxa Broadcast Scan

Omron

- FINS Discovery

Red Lion

- Sixnet Discovery

Schneider

- Schneider Netmanage Discovery

SMA

- Speedwire Discovery

Ubiquiti

- Ubiquiti Broadcast Scan

Welding Technology Corporation (WTC)

- Raft Gateway Discovery

Westermo

- WeConfig Discovery

Zebra

- Printer Discovery

Edge 3.6 版本支持 Windows 7 单播查询

ABB

- MMS
- Modbus

American Power

- FTP

Andover

- SNMP

Anord Mardix

- HTTP

Atlas Copco

- Atlas Open Protocol
- MWR
- HTTP

American Power

- FTP

Axis

- FTP

B&R

- HTTP
- SNMP
- NBNS

Beckhoff

- Beckhoff

Beijer (Mitsubishi)

- Beijer

Bosch

- Indraworks

Brightwell

- Brightwell DBTalk

Brother

- HTTP

Cognex

- Cognex

CTI

- CTI

Dallmeier

- HTTP

Danfoss

- Modbus

Digiboard

- HTTP

Emerson

- Telnet

Enterasys

- SNMP (v1)

EXI

- Exi 3000

Fanuc

- CIP
- FOCAS

Fisher-Rosemount

- Telnet

Fuji-Xerox

- HTTP

GE

- GESRTP

Grandstram

- HTTP

Hikvision

- HTTP

Hirschmann

- Telnet

HMS

- EN/IP

HP

- HTTP
- NBNS

Hikvision

- SADP

Impinj

- SNMP

Janitza

- SNMP
- HTTP

Johnson Controls

- BACNET

Keyence

- CIP

Lantronix

- Lantronix

Lantronix

- Telnet

Microsoft

- NBNS

Mitsubishi

- Melsoft
- Mitsubishi GOT

Mobotix

- HTTP

Moxa

- Moxa Unicast Scan
- Telnet

Omron

- EN/IP
- FINS

Opto-22

- OPTO

Philips

- HTTP

Phoenix

- HTTP

Polycom

- HTTP

Prosoft

- CIP

Red Lion

- CIP
- HTTP
- Sixnet Query

Ricoh

- SNMP

Rockwell

- CIP

RouterBOARD (MikroTik)

- HTTP

RS

- CIP

Schneider

- UMAS (Schneider Modbus)
- HTTPS
- Modbus

Schweitzer Engineering Laboratories:

- Telnet
- DNP3
- MMS Query

SEW Eurodrive

- CIP

SICK

- EN/IP

Siemens

- MMS
- S7 - SNMP
- Sinumerik
- Siprotec5 (HTTP)
- SNMP

Sierra Monitor

- EN/IP

Sigmatek

- BACnet

SMA Solar Technology

- Speedwire

Square D

- Modbus

Synology

- HTTP

TAC-AB

- SNMP

Teltonika

- SNMP

Terasaki

- Modbus

Texas Instruments

- Brightwell DBTalk Query

TP-Link

- HTTP

Tridium

- Tridium Fox

Ubiquiti

- Ubiquiti

Universal Global Scientific Industrial

- Moxa Unicast Scan

- Telnet

WAGO

- EN/IP
- WAGO

Westermo

- SNMP
- Telnet

Welding Technology Corporation (WTC)

- Raft Gateway Discovery

Yaskawa Electric

- FTP

Zebra

- SNMP

Edge 3.6 版本支持项目文件 (Project Files)

下表列出了 Edge 可以在主机上自动检测的、支持的文件格式。

项目文件类型 (Project File Type)	文件扩展名 (File Extension)
SEL	*.rdb
Siemens DIGSI V4	*.zip
Omron Sysmac Studio	*.smc2
Toyoda PCwin	*.zip
Rockwell Harmony	*.rsh
Rockwell Studio 5000	*.acd
Schneider Electric EcoStruxure	*.zip, *.xbk
Siemens Step7 v5	*.zip
Siemens TIA Portal v13-19	*.zip, *.zap13-19
Siemens TIA Portal	*.zip
Schneider UnityPro	*.stu
Yokogawa CentumVP	*.zip

在指定目录中手动检测 ICS 项目文件

以下是 Edge 可以解析的供应商和协议, 前提是用户提供了它们的目录路径:

Standard

- SCL

ABB

- 800xA
- AC800M
- Advant
- Composer
- RTU5XX SCADAVantage

- Totalflow PCCU

Beckhoff

- TwinCAT3

B&R

- Automation Studio v3/v4

CODESYS

- CodesysV3

Emmerson

- DeltaV

Fuji

- SX-Programmer (D300Win)

GE

- Bently Nevada
3500 System Configuration
- MarkVI ToolBoxST
- rx3i,9030 Proficy Machine
- rx3i,9030 PacsAnalyzer

Honeywell

- EHPM
- Experion Ctools / SIT

Kepware

- Kepware OPC

Kuka

- Robots

LS

- XG5000

Mitsubishi

- GX Works2
- GX Works3
- Melsec GX Developer
- DIASYS Netmation

Motorola

- ACE, MOSCAD ACE3600

Omron

- CX-One
- Sysmac Studio

Red Lion

- Red Lion HMIs Crimson
v3.0/3.1

Rockwell

- AAdvance Log Collection
- AssetCentre
- FactoryTalkView / RSView
- ICSTriplex Log Collection
- ISaGRAF (multiple)
- MicroLogix Factory View
- MicroLogix RS System
Ferret
- RSLogix 5000 / 500 / 5
- RSLinx
- Trusted TMR IEC 1131
Toolset

Schneider

- Concept
- EcoStruxure Building Ops
- M221 SoMachine
- Modicon/Quantum
- SCADAPack 32 Telespace
Studio

- TSX Micro, Premium PL7
- TwidoSuite
- GP-3000 GP-Pro EX
- GP-4000 GP-Pro EX
- LT-3000 GP-Pro EX
- LT-4000 GP-Pro EX
- IPC (PC/AT)
- SP-5000 GP-Pro EX
- ST-3000 IPC (PC/AT) GP-
Pro EX

SEL

- AcSELerator
- AcSELerator QuickSet
- AcSELerator RTAC

SICK

- Sopas ET

Siemens

- LOGO!Soft Comfort
- PCS7
- Proneta
- S7 TiaPortal
(v13/v14/v15/v16/v17/
v18,v19)
- S7/T3000 Step7
- Simatic Softshop 505
- Siprotec Digsig4 / Digsig5

- TIA Portal Project Server

Toyoda

- PCWin

Triconex

- Tricon/Trident/TriGP

- TriStation 1131

Xinje

- Xinje PLCs XDPPro

Yokogawa

- Centum VP/CS3000