

Industrial Security Appliance 3000 Data Sheet

Developed specifically to withstand the harshest industrial environments, these industrial firewalls offer uncompromising end to end security with industrial design and operation in mind.

Product Overview

The Cisco® Industrial Security Appliances are true industrial firewalls that provide OT targeted protection based on proven enterprise class security.

The ISA 3000 with four data links is a DIN rail mount, ruggedized appliance that provides the widest range of Access, Threat, and Application controls for the harshest and most demanding of industrial environments.

The ISA 3000 Series starts with the same industrial success of the IE 4000 switch hardware design and adds the proven security of the Cisco ASA firewall and Source Fire Next Generation IPS software. The ISA 3000 is the answer to provide both safety and security to your network modernization projects. It also provides the anchor point for converging IT and OT security visibility without interfering with industrial operational practice. This security appliance is built to withstand extreme environments, reflect industrial design, all the while adhering to overall IT network design, compliance, and performance requirements.

The ISA 3000 Series is ideal for industrial Ethernet applications where hardened products are required. The product is successfully running in major electrical utilities, energy production, mining and other automation environments. Further uses are intelligent transportation systems (ITS), city surveillance programs, and water/wastewater utilities. Security and safety visibility has never been higher with the ability to simultaneously track suspect file propagation, coil set points, abnormal traffic patterns, and escalation of privileges all within a single device. This industrial element of Cisco's secure networking portfolio cooperatively interacts with other industrial grade Cisco solutions as well as provides complete vision to interactions between your local cell, the IT world, outside vendors, or contractor activity.

Proper deployment of the ISA 3000 industrial firewall can fulfill security requirements associated with a variety of industrial standards, regulations, and guidelines such as: NERC-CIP, ISA 99, ISA 62443, CFATS, ANSI/AWWA G430 and others.

Managed through either a user-friendly on-box system manager or company wide security management, the ISA 3000 provides industrial focused, out-of-the-box configuration and simplified operational manageability. These highly customizable management options allows for simplified local operational awareness and higher order IT/OT security convergence for the inevitable mingling of industrial and IT capabilities.

Table 1. Capabilities of Cisco ISA 3000

Robust Industrial Design	<ul style="list-style-type: none"> • Built for harsh environment and temperature range (-40° to 70°C). • Hardened for vibration, shock, surge, and electrical noise immunity. • Four 1 Gigabit Ethernet uplink ports provide multiple resilient design options.(4 copper or 2 copper plus 2 fiber) • Complies with multi-industry specifications for industrial automation, ITS, and electrical substation environments. • Improves uptime, performance, and safety of industrial systems and equipment. • Compact DIN rail unit design with industrial LED features allowing easy monitoring. • Fanless, convection cooled with no moving parts for extended durability. • IEEE 1588v2 PTP (both power profile and default profile are supported). • Alarm I/O for monitoring and signaling to external equipment.
User-Friendly GUI Device Manager	<ul style="list-style-type: none"> • On-device management for local awareness immediate control. • Multi-device management can handle 100s of devices • User specific access and control customizations.
Traffic Continuity/Protection	<ul style="list-style-type: none"> • Full “lights out” traffic bypass copper ports. • Default passive deployment learning mode. • Software updates possible without traffic loss. • Connection limitations protect from DOS causing traffic. • Latency detection and mitigation functions. • Quality of Service policies
Proven, Extensible Access Control	<ul style="list-style-type: none"> • Enforces ISA-95/IEC 62264 segmentation needs • Full stateful inspection • Layer 2 and Layer 3 Firewall operation modes • Downloadable Access Control Lists • Identity based access control policies • Users/User Groups • Policy based routing ACLs • Extended ACLs • WebVPN ACLs • Dynamic ACLs • TrustSec ACLs
Uncompromising Threat Detection	<ul style="list-style-type: none"> • Over 25,000 rules provide the widest range of protection anywhere • Hundreds of industrial focused rules. • Industrial equipment exploit protection rules • Protocol abuse identification • Protects web based control systems • Network behavior analytics • Passive device discovery
Application Control	<ul style="list-style-type: none"> • Visibility and Control of all DMZ infrastructure • Visibility and Control of Industrial applications • Visibility and Control of individual protocol commands and values • Example Protocols Addressed for Visibility and/or Control: BACnet; CIP; COSEM; DNP3; EtherIP; GOOSE; IEC 60870-5-104; ISO-MMS; Modbus; OPC-UA;
Remote Access Enablement/Controls	<ul style="list-style-type: none"> • Network Access Control via Cisco AnyConnect • Identity Services Engine support • Site to Site VPN • Remote Access VPN • Clientless SSL VPN offering • Cisco Secure Desktop • Support for Citrix and VMware clientless connections
DMZ Infrastructure	<ul style="list-style-type: none"> • DNS Services • DHCP Services • AAA Support • IP Routing

Your Ruggedized Choice for Industrial Firewall Deployments

The Cisco Industrial Security Appliance 3000 Series offer:

- Controlled access from cell and substation level all the way up to ISP connectivity.
- Flexible, enterprise class remote access.
- Provides basic network infrastructure services such as DNS and DHCP.
- Unequaled threat protection for every level of networking and computing - from the switch, router, OS, compute infrastructure, to industrial control systems.
- More levels of traffic continuity safety than other offering in the industrial space.
- Application visibility and control for every level of application in the industrial and enterprise space.

Figure 1 shows the ISA 3000, Table 2 shows the available ISA 3000 ordering PIDs, and Table 3 lists the SFP modules for Cisco Industrial Security Appliance 3000 Series.



Table 2. Cisco Industrial Security Appliance 3000 Series Models and options:

Product Number	Copper 10/100/1000 (all bypass enabled)	SFP Fiber Ports
ISA-3000-2C2F-K9	2	2
ISA-3000-4C-K9	4	0
Optional Orderable Features		
L-ISA3000SEC+-K9		HA enablement, SSL VPN, greater connection count, VLAN trunking
L-ISA3000-TA=		Threat/Application Subscription License
L-ISA3000-TA-1Y		1 Year Subscription Threat/Application
L-ISA3000-TA-3Y		3 Year Subscription Threat/Application
L-ISA3000-TA-5Y		5 Year Subscription Threat/Application

Table 3. Supported Cisco Ruggedized SFPs

Product Number	Type
GLC-SX-MM-RGD=	1000 BASE-SX Ruggedized
GLC-LX-SM-RGD=	1000 BASE-LX/LH Ruggedized
GLC-FE-100FX-RGD=	100 BASE-FX Ruggedized
GLC-FE-100LX-RGD=	100 BASE-LX Ruggedized

Product Specifications

Table 4 lists physical specifications, Table 5 gives information about device performance and scalability, Tables 6 and 7 list some important software features, Table 8 lists compliance specifications, and Table 9 gives information about management and standards of the Cisco ISA 3000 Series

Table 4. Physical Product Specifications

Description	Specification
Hardware	<ul style="list-style-type: none"> • 4 Core Intel Rangely (I-temp) • 8-GB DRAM (soldered down) • 16-GB onboard flash memory • mSATA 64Gb • 1-GB removable SD flash memory card - industrial temp (enabled in future release) • Mini-USB connector for console • RJ-45 traditional console connector • Dedicated 10/100/1000 Management port • Hardware based anti-counterfeit, anti-tamper chip • Factory reset option
Alarm	<ul style="list-style-type: none"> • Alarm I/O: two alarm inputs to detect dry contact open or closed, one Form C alarm output relay
Dimensions, (H x W x D)	<ul style="list-style-type: none"> • 11.2cm (Width) x 13cm (Height) x 16cm (Depth)
Weight	<ul style="list-style-type: none"> • 1.9kg
Power Supply and Ranges	<ul style="list-style-type: none"> • Dual internal DC • Nominal \pm 12Vdc, 24Vdc, or 48Vdc • Maximum Range 9.6 Vdc to 60 Vdc • Power Consumption 24 Watts
MTBF - Mean Time Between Failure	<ul style="list-style-type: none"> • ISA-3000-4C 398,130 hours • ISA-3000-2C2F 376,580 hours

Table 5. Device Scalability

Description	Specification
Throughput	Max 2Gbps - Min. 22Mbps Varies with traffic type and security activity (please work with Cisco SE for your traffic profile)
IPSec VPN Tunnels	5, 25 (with SecPlus license)
Defined Interfaces	200, 400 (with SecPlus license)
VLAN counts	5, 25 (with SecPlus license)
IPv4 MAC security ACEs	1,000 with default TCAM Template
NAT translation	Bidirectional, 128 unique subnet NAT translation entries, which can expand to tens of thousands of translated entries if designed properly

Table 6. Cisco ISA 3000 Key Network Support Features

General Features	Features
NAT	<ul style="list-style-type: none"> • Static NAT • With Port Translation, One-to-Many, Non-standard ports • Dynamic NAT • Dynamic PAT • Identity NAT
Layer 2 IPv6	IPv6 Host support, HTTP over IPv6, SNMP over IPv6
Layer 3 Routing	IPv4 Static Routing Dynamic Routing - RIP, EIGRP, ISIS, OSPF & BGP

General Features	Features
Utility	IEEE 1588 (PTP HW enabled)
Separate Routing for Management Traffic	Segregates data and management traffic routing
Trunking	802.1q trunks supported

Table 7. Cisco ISA 3000 Key Security Software Features

Security Area	Features
TrustSec Controls	<ul style="list-style-type: none"> • In-band and out of band Identity • Active Directory integration • Policy based on Security Group Tags • 802.1x support • MACSec and MAB support • Enforces end-point security state for remote access
Multi-Level Access Controls	<ul style="list-style-type: none"> • Global Blacklists - automated or manual • Global Whitelists • Third party intelligence feed utilization • File Whitelists • File Blacklists • Application level access control • 802.1x support
Threat Network Mapping	<ul style="list-style-type: none"> • Passive device identification • Mobile device identification • Application host network mapping • Vulnerability/host network mapping • User/host network mapping
Threat Discovery	<ul style="list-style-type: none"> • Indicators of Compromise tracking • OpenAppID - open community ID system • Correlation policies and responses • Traffic variance detection • Router based remediation actions • Netflow tracking • 25,000+ threat identifiers • Customizable identifiers • Can create wholly new identifiers • Widest identifier contributorship
File Tracking	<ul style="list-style-type: none"> • Approved file trace • Suspect file trace • Malware match

Table 8. Compliance Specifications

Type	Standards
Electromagnetic Emissions	FCC 47 CFR Part 15 Class A EN 55022A Class A VCCI Class A AS/NZS CISPR 22 Class A CISPR 11 Class A CISPR 22 Class A ICES 003 Class A CNS13438 Class A KN22

Type	Standards
Electromagnetic Immunity	EN55024 CISPR 24 AS/NZS CISPR 24 KN24 EN 61000-4-2 Electro Static Discharge EN 61000-4-3 Radiated RF EN 61000-4-4 Electromagnetic Fast Transients EN 61000-4-5 Surge EN 61000-4-6 Conducted RF EN 61000-4-8 Power Frequency Magnetic Field EN 61000-4-9 Pulse Magnetic Field EN 61000-4-18 Damped Oscillatory Wave EN-61000-4-29 DC Voltage Dips and Interruptions
Industry Standards	EN 61000-6-1 Immunity for Light Industrial Environments EN 61000-6-2 Immunity for Industrial Environments EN 61000-6-4 Emission Standard for Industrial Environments EN 61326 Industrial Control EN 61131-2 Programmable Controllers IEEE 1613 Electric Power Stations Communications Networking IEC 61850-3 Electric Substations Communications Networking NEMA TS-2 EN 50121-3-2 EN 50121-4 EN 50155
Safety Standards and Certifications	Information Technology Equipment: UL/CSA 60950-1 EN 60950-1 CB to IEC 60950-1 with all country deviations NOM to NOM-019-SCFI (through partners and distributor) Industrial Floor (Control Equipment): UL 508 CSA C22.2, No 142 EN/IEC 61010-2-201 UL/CSA 61010-1 Hazardous Locations* ANSI/ISA 12.12.01 (Class I, Div 2 A-D) CSA C22.2 No 213 (Class 1, Div 2 A-D) UL/CSA 60079-0, -15 IEC 60079-0, -15 (IECEx test report Class I, Zone 2, group II gases) EN 60079-0, -15 ATEX certification (Class I, Zone 2, group II gases) *Must meet deployment requirements such as with IP 54 enclosure described in the following document: Product Documentation and Compliance Information for the Cisco ISA 3000 Industrial Security Appliance http://www.cisco.com/c/dam/en/us/td/docs/security/Firewalls/ISA3000/ISA3000-PDOC.pdf
Operating Environment	Operating Temperature: -40C to +74C <ul style="list-style-type: none"> • -40C to +70C (Vented Enclosure Operating) • -40C to +60C (Sealed Enclosure Operating) • -40C to +75C (Fan or Blower equipped Enclosure Operating) EN 60068-2-21 EN 60068-2-2 EN 61163

Type	Standards
Storage Environment	Temperature: -40 to +85 degrees C Altitude: 0-15,000 feet IEC 60068-2-14
Humidity	Relative humidity of 5% to 95% non-condensing. IEC 60068-2-30
Shock and Vibration	<ul style="list-style-type: none"> • IEC60068-2-6 and IEC60068-2-27 • MIL-STD-810, Method 514.4 • Marine EN60945 • Industrial EN61131-2/IEC61131-2 • Railway EN61373 CAT 1B • Smart Grid EN61850-3 • IEEE 1613
Corrosion	ISO 9223: Corrosion class C3-Medium class C4-High EN 60068-2-52 (Salt Fog) EN 60068-2-60 (Flowing Mixed Gas)
Others	RoHS Compliance China RoHS Compliance TAA (Government) CE (Europe)
Warranty	Five-year limited HW warranty on all ISA 3000 PIDS. See link at end of Datasheet for more details on warranty.

Table 9. Management and Standards

Description	Specification	
IEEE Standards	<ul style="list-style-type: none"> • IEEE 802.1D MAC Bridges, STP • IEEE 802.1p Layer2 COS prioritization • IEEE 802.1q VLAN • IEEE 802.1s Multiple Spanning-Trees • IEEE 802.1w Rapid Spanning-Tree • IEEE 802.1x Port Access Authentication • IEEE 802.1AB LLDP • IEEE 802.3ad Link Aggregation (LACP) 	<ul style="list-style-type: none"> • IEEE 802.3ah 100BASE-X SMF/MMF only • IEEE 802.3x full duplex on 10BASE-T • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification • IEEE 1588v2 PTP Precision Time Protocol
RFC Compliance	<ul style="list-style-type: none"> • RFC 768: UDP • RFC 783: TFTP • RFC 791: IPv4 protocol • RFC 792: ICMP • RFC 793: TCP • RFC 826: ARP • RFC 854: Telnet • RFC 951: BOOTP • RFC 959: FTP • RFC 1157: SNMPv1 • RFC 1901,1902-1907 SNMPv2 • RFC 2273-2275: SNMPv3 • RFC 2571: SNMP Management • RFC 1166: IP Addresses • RFC 1256: ICMP Router Discovery 	<ul style="list-style-type: none"> • RFC 1305: NTP • RFC 1492: TACACS+ • RFC 1493: Bridge MIB Objects • RFC 1534: DHCP and BOOTP interoperation • RFC 1542: Bootstrap Protocol • RFC 1643: Ethernet Interface MIB • RFC 1757: RMON • RFC 2068: HTTP • RFC 2131, 2132: DHCP • RFC 2236: IGMP v2 • RFC 3376: IGMP v3 • RFC 2474: DiffServ Precedence • RFC 3046: DHCP Relay Agent Information Option • RFC 3580: 802.1x RADIUS • RFC 4250-4252 SSH Protocol

¹ For the complete list of the supported SFP models, please refer to http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html.

² MMF = multi-mode fiber

³ SMF = single-mode fiber

Warranty Information

Warranty information for the ISA 3000 is available at <http://www.cisco-servicefinder.com/warrantyfinder.aspx>

Cisco and Partner Services

At Cisco, we're committed to minimizing our customers' TCO, and we offer a wide range of services programs to accelerate customer success. Our innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services helps you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Some of the key benefits our customers can get from Cisco Services follow:

- Mitigating risks by enabling proactive or expedited problem resolution
- Lowering TCO by taking advantage of Cisco expertise and knowledge
- Minimizing network downtime
- Supplementing your existing support staff so they can focus on additional productive activities

For more information about Cisco Services, refer to Cisco Technical Support Services or Cisco Advanced Services at <http://www.cisco.com/web/services/>.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)

For More Information

For more information about the Cisco ISA 3000 Series, visit <http://www.cisco.com/go/isa3000> contact your local account representative.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed at the Information Technology Division, US Naval Research Laboratory. This product includes software developed at the University of California, Irvine for use in the DAV Explorer project (<http://www.ics.uci.edu/~webdav/>). This product includes software developed by Boris Popov. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). This product includes software written by Tim Hudson (tjh@cryptsoft.com).




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 www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)