PacStar®
Imagined. Engineered. Delivered.™

CURTISS-WRIGHT

PacStar Enterprise CSfC Solutions (ECS)

Curtiss-Wright PacStar Enterprise CSfC Solutions (ECS) provide gateway services for classified networks using enterprise-class COTS products to meet the security and configuration requirements of the National Security Agency (NSA) Commercial Solutions for Classified (CSfC) program. PacStar ECS enable DoD and Federal organizations to transmit classified information over untrusted networks, using commercial encryption components. PacStar ECS enable executive mobility and remote work (e.g., using laptops and smartphones), site-to-site extensions of classified networks (e.g., for remote tactical teams, branch offices, home offices, or multi-building campuses), and classified campus-area Wi-Fi networks.

PacStar ECS are a family of gateway solutions that scale from small installations with less than 100 secure connections to large enterprise-class services supporting thousands of concurrent users. PacStar ECS designs are based on our extensive experience developing tactical CSfC solutions, are fully supported by Curtiss-Wright expert CSfC network and cybersecurity engineers and can be customized to meet program requirements.

PacStar ECS enable rapid implementation of CSfC solutions, lowering costs and reducing risk because they are based on fully integrated, tested, and proven solutions. PacStar ECS are managed by PacStar IQ-Core® Software to simplify maintenance, unify management, reduce complexity, decrease downtime, and shorten training for PacStar ECS administrators.

PacStar ECS significantly reduce equipment costs compared to Type 1 encryption hardware and enable U.S. Coalition Partner interoperability – all without using controlled cryptographic items (CCI).

Key Benefits

Reduced Complexity
Built on industry-leading networking technology and using a repeatable, proven, reference network design; will simplify integration, testing, training, and support

Compatibility
Networking technology and capabilities provide maximum compatibility with DoD and coalition networks

Compliance
Core networking, encryption, and PKI technologies integrated into PacStar ECS are Common Criteria and FIPS certified

Security
Ensures maximum security by using enterprise-class technology from the most widely deployed cybersecurity industry partners in the U.S. DoD

Manageability
PacStar IQ-Core Software reduces system complexity and simplifies management for system and cybersecurity administrators

Solutions Architecture

PacStar ECS, combined with PacStar technical expertise, integration, testing, and certification experience, deliver CSfC networking solutions for fixed installations, using enterprise COTS rack-mount equipment.

PacStar ECS use independent, layered COTS products and Commercial National Security Algorithm (CNSA) suites of cryptographic algorithms to protect classified National Security Systems (NSS) data-in-transit up to the Top Secret level.

PacStar ECS architectures include components necessary to meet infrastructure requirements for all NSA CSfC capability packages and appendices, including:

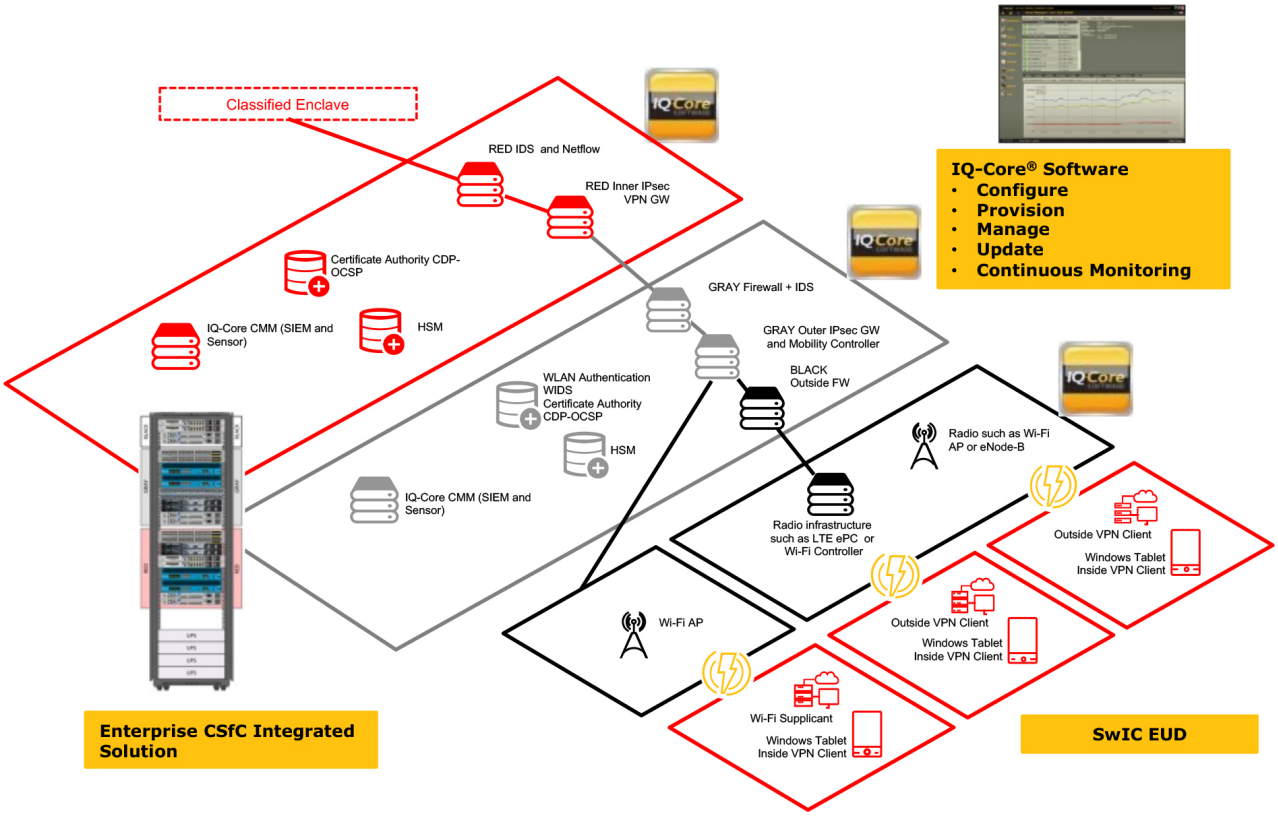
- Authentication servers
- Inner VPN gateways and encryption components
- Outer VPN gateways and encryption components, including WLAN controllers
- Intrusion detection / prevention systems, including Wireless IDS
- Traffic filtering firewalls
- Security incident and event managers, network IDS and flow collectors
- Public key infrastructure (PKI), including certificate authorities, hardware security modules, OCSP/CDPs
- Network Services (Domain Services, NTP servers, etc.)

PacStar IQ-Core® Software, including IQ-Core Network Communications Manager (NCM), IQ-Core Crypto Manager (CM) and IQ-Core Continuous Monitoring Manager are used within PacStar ECS to simplify and unify configuration management, situational awareness, and real-time monitoring.

- **Faster Provisioning:** PacStar IQ-Core Software management framework is purpose-built for rapid provisioning and activating EUDs at scale. The typical times for manually provisioning an EUD is several hours – provisioning the EUD using PacStar IQ-Core Software can be accomplished in as little as 7 minutes.
- **Efficient Certificate Management:** PacStar IQ-Core Software has a vendor-neutral GUI (i.e., supports ISC, Red Hat) and tools for creating, signing, distributing, renewing and revoking certificates. Using PacStar IQ-Core Software, EUDs certificate management is performed over-the-air.
- **Automated Updates:** The PacStar IQ-Core Software "check-in" process keeps track of software patches, configuration changes and certificates and proactively pushes out updates to the EUDs in the background and without interruption to the user experience. The EUD updates are fine-grained and only apply to specific components that require and update hence conserving bandwidth and data usage.

This architecture allows multiple simultaneous transports to be supported without additional changes in the encryption scheme. Transports can include terrestrial circuits, Wi-Fi, cellular, satellite, etc. Additionally, multiple security domains can share transports with separate red networks supported with additional CSfC components.

Solutions Architecture (continued)

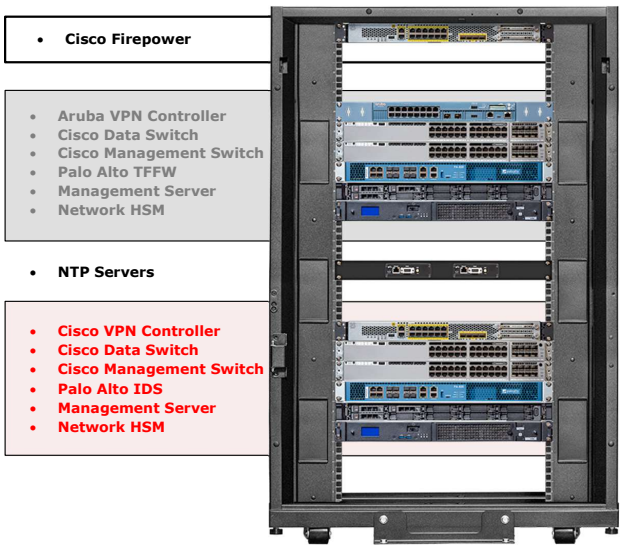


Example Logical Network for Mobile Access Capability Package Solution

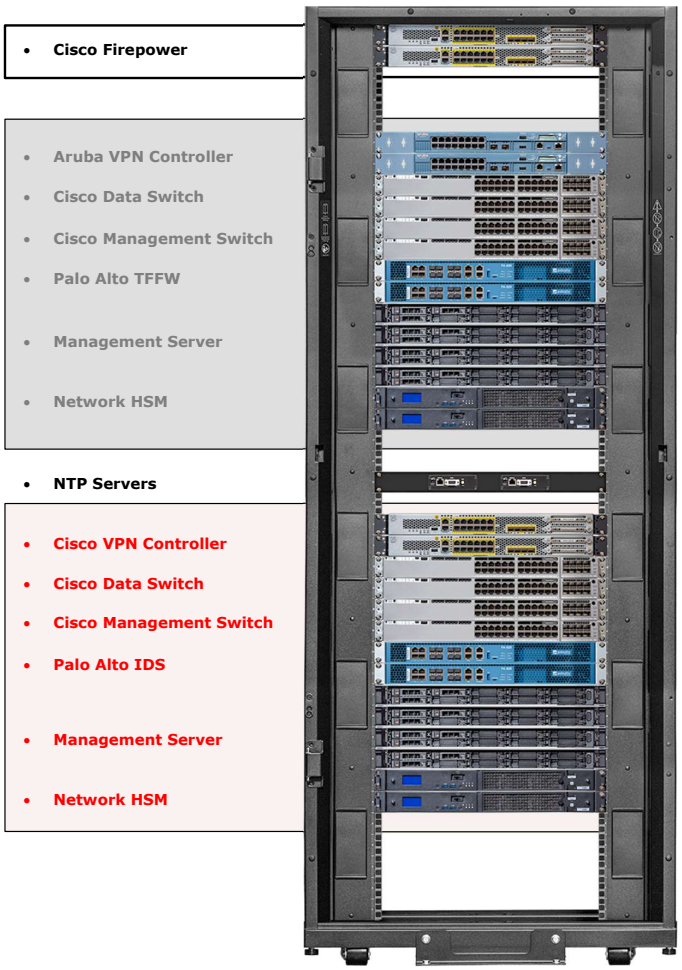
PacStar ECS Key Features

- Complete, integrated hardware and software infrastructure configured to meet the CSfC Capability Packages and Appendices for Data-in-Transit
- Technologies listed on the DoDIN APL, NIAP/Common Criteria, FIPS/CMVP and CSfC Approved Components lists
- Enterprise Class Commercial Hardware Appliances
  - 19" rackmount hardware
- Scalable options:
  - Small installation ≤ 100 concurrent connections
  - Large installation (with high availability) ≤ 5000 concurrent connections
- High-throughput IPsec/VPN gateways, traffic filtering firewalls, intrusion detection systems
  - 10 GigE network backbone for large installations
  - 1 GigE network backbone for small installations
- Turn-key implementation and experienced technical support

PacStar Enterprise CSfC Solutions (Gateway Proof of Concept)



PacStar Enterprise CSfC Solutions (Mobile Access Gateway with High Availability)



Supported CSfC Component Vendors

Curtiss-Wright collaborates closely with industry-leading, enterprise-class makers of networking, encryption, and cybersecurity technologies – integrating, testing, and delivering their technologies integrated in PacStar ECS, including:PacStar IQ-Core CMM customers benefit from Elastic technologies because embedded Elastic technologies:

CSfC Components	Vendors*
Authentication Servers	HPE Aruba ClearPass Policy Manager
Certificate Authorities	ISC CertAgent, Red Hat Certificate Services, Windows ADCS
Continuous Monitoring / SIEMs	PacStar IQ-Core Continuous Monitoring Manager w/Elastic
End User Device Management	Integrity Global Security INTEGRITY, Forcepoint Trusted Thin Client
Hardware Security Modules	Thales Luna
IPsec VPN Gateways	HPE Aruba Mobility Controller, Cisco ASA/Firepower/IOS-XE Routers, Juniper SRX
Network Time Protocol Servers	TimeMachines
Traffic Filtering Firewalls	Cisco ASA/Firepower, Palo Alto NGFW, Juniper SRX
Wireless Intrusion Detection / Prevention Systems	HPE Aruba Airwave
Server Virtualization	VMware ESXi, vSphere, Horizon

*Complete solutions include servers, routers, switching, storage, and power solutions from leading enterprise IT vendors which are out of scope of CSfC specifications.

Curtiss-Wright integrates and supports technologies from additional 3rd parties, into tactical CSfC integrated solutions that provide remote access when paired with PacStar ECS. See Curtiss-Wright's family of tactical CSfC solutions for more details.

Supported CSfC Architectures

Curtiss-Wright offers complete, turnkey, integrated hardware and software infrastructure configured to meet the CSfC Capability Packages and Appendixes to protect data-in-transit, including:

- Mobile Access Capability Package: Providing gateway and cybersecurity solutions enabling classified mobile devices to communicate over untrusted networks.
- Multi-Site Connectivity Capability Package: Providing gateway and cybersecurity solutions enabling remote teams or branch offices, each with their own networks, to communicate over untrusted networks.
- Campus Wireless LAN Capability Package: Providing Wi-Fi and cybersecurity infrastructure enabling mobility for classified Wi-Fi devices within a facility or command post.
- Enterprise Gray Annex: Providing combined infrastructure enabling multiple capability packages and networks to share a single gray network and centralized cybersecurity suite.
- Key Management Annex: Providing key management and PKI technologies and processes enabling certificate or pre-shared key encryption management.
- Continuous Monitoring Annex: Providing data collection and management enabling cybersecurity monitoring of CSfC Solutions.
- Wireless Intrusion Detection System / IPS Annex: Providing Wi-Fi monitoring, alerting and defense, enabling wireless infrastructure security.

PacStar IQ-Core® Software for PacStar ECS

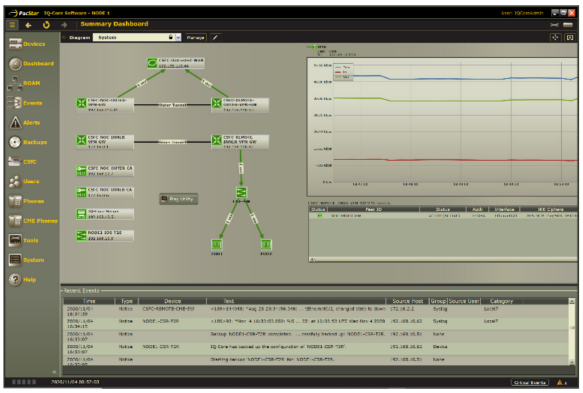
Because CSfC systems require two independent encryption systems including PKI, from two different vendors or platforms, they add complexity and training burden on organizations. IQ-Core Software overcomes the added complexity and training burden by simplifying the setup, configuration and management of the underlying equipment used in CSfC solutions:

- Enabling the deployment of CSfC solutions, with attendant benefits, while reducing the amount of added complexity and training
- Providing a unified interface to underlying equipment from multiple vendors
- Providing means to monitor multiple sets of equipment, in fixed/branch office and deployed settings, so that operators can manage the equipment at remote sites

PacStar IQ-Core Software comprises a family of software editions designed to address common challenges in managing systems consistent of equipment and software from multiple vendors. The editions include IQ-Core Network Communications Manager (NCM), IQ-Core Crypto Manager (CM) and IQ-Core Continuous Monitoring Manager (CMM) and IQ-Core Remote Operations and Management (ROAM). They work together providing advanced, unified management of PacStar ECS.

PacStar IQ-Core Crypto Manager (CM)

PacStar IQ-Core CM is purpose-built to manage CSfC solutions.



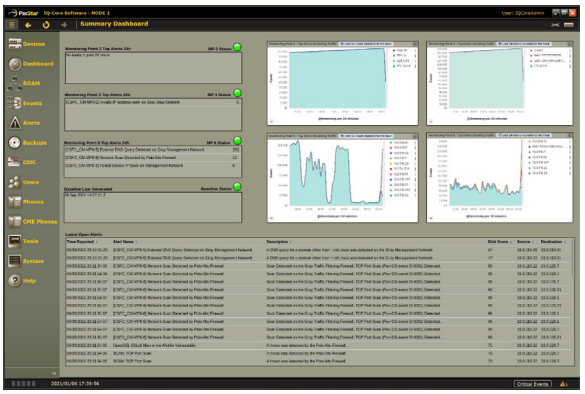
PacStar IQ-Core CM:

- Saves time by automating complex, time-consuming, and error-prone tasks such as VPN set-up, with powerful wizards with common user interfaces across hardware, software, and PKI components
- Provides cyber situational awareness (SA) by securing and consolidating alerting information for all components of a CSfC solution. It provides enhanced CSfC SA at the core and edge of the network with extensive real-time status of crypto tunnels, certificate expiration alerts, and connection auditing
- Streamlines innovation by interoperating with a broad range of enterprise CSfC-certified communications hardware and systems, simplifying upgrades, and adoption of new COTS technologies
- Facilitates remote and distributed management through the ability to perform CSfC-related management tasks from anywhere in the world
- Large scale EUD provisioning, monitoring, over-the-air updates for certificate management and software patching

PacStar IQ-Core CM assists organizations in meeting Key Management Requirements for CSfC systems and dramatically simplifies the error-prone process of issuing, managing, and renewing the PKI certificates.

PacStar IQ-Core Continuous Monitoring Manager (CMM)

PacStar IQ-Core CMM is a turnkey solution that includes technologies pre-configured to meet CSfC Continuous Monitoring Annex requirements for network infrastructure.



PacStar IQ-Core CMM:

- Is based on industry-leading, proven, secure and scalable technology from Elastic.
- Is pre-configured to meet STIG, NIST and CSfC requirements for security
- Provides easy-to-understand, pre-configured dashboards and alerts
- Addresses required SIEM requirements and monitoring points for infrastructure.
- Is integrated into and optimized for PacStar ECS

PacStar IQ-Core Network Communications Manager (NCM)

PacStar IQ-Core NCM is the core IQ-Core Software platform, designed to manage network and cybersecurity technologies.

PacStar IQ-Core NCM:

- **Provides an intuitive user interface:** Makes communications set-up and operation quick and easy to learn and recall. Includes customizable user interfaces and roles-based access control, providing tailorable access to features depending on user experience level. This reduces training time and costs.
- **Reduces configuration errors:** Assists organizations in maintaining uptime, performance, and compliance with cyber security requirements
- **Simplifies troubleshooting:** Through integrated tools for both entry-level and advanced network administrators, reducing reliance on contract field service representatives
- **Saves time:** Automates complex, time-consuming, and error-prone tasks with powerful wizards with common user interfaces across hardware and software components
- **Provides cyber situational awareness (SA):** Enhanced network and cyber SA at the core and edge of the network with extensive real-time status, alerts, and auditing
- **Facilitates remote and distributed management:** Ability to monitor, change device configurations and troubleshoot from anywhere in the world
- **Streamlines innovation:** Interoperates with a broad range of the most popular enterprise communications hardware, systems, and protocols -- streamlining upgrades and adoption of new COTS technologies at the edge

PacStar IQ-Core Remote Operations and Management (ROAM)

PacStar IQ-Core ROAM integrates with IQ-Core Network Communications Manager (NCM) and IQ-Core Crypto Manager (CM) to offer a comprehensive suite of capabilities across distributed networks. IQ-Core ROAM can run at any tier and any node in a network, and adds the following capabilities:

- **Saves time** by enabling visibility of status across all network nodes, at-a-glance. Enables bulk updates of all network nodes from a single interface.
- **Provides cyber situational awareness** by securing, consolidating, and forwarding alerting information at each tier of the tactical network. Provides enhanced network situational awareness at the core and edge of the tactical networks, with extensive real-time visibility of connected nodes. Operates seamlessly in a disconnected, intermittent, and limited (DIL) environment.
- **Facilitates remote and distributed management** by enabling upper echelon administrators to interoperate with and assist remote operators. Enables remote operators to perform all tasks, even when they have no WAN connectivity.
- **Field-proven,** based on the widely deployed PacStar IQ-Core NCM communications management platform