PacStar IQ-Core EUDM

End User Device Manager (EUDM)

Curtiss-Wright's PacStar® IQ-Core® End User Device Manager (EUDM) automates provisioning, configuring, and updating of end user devices (EUDs) for classified networks, meeting the security and configuration requirements of the National Security Agency (NSA) Commercial Solutions for Classified (CSfC) program.

Combined with Dell or HP laptops and the Secured with INTEGRITY client (SwIC) from INTEGRITY Global Security (IGS), PacStar IQ-Core EUDM enables federal defense and civilian organizations to manage EUDs approved to transmit classified information over untrusted networks.

The NSA CSfC Mobile Access Capabilities Package (MACP) specifies how federal organizations can configure and deploy mobile devices to meet security requirements necessary for classified access, enabling executive mobility and remote access. To minimize the size, weight, power, cost (SWaP-C), and complexity of meeting these security requirements, organizations can use appropriately configured virtual machine-separated VPN clients running on mobile devices. While this configuration is ideal for mobility, it introduces technology complexity far above standard EUDs that must be automated to ensure uptime and reduce administrative and management workloads.

PacStar IQ-Core EUDM works with Curtiss-Wright's PacStar Enterprise CSfC Solutions (ECS) as well as PacStar tactical CSfC solutions to create end-to-end, managed CSfC solutions from the leading provider of proven CSfC technologies. PacStar ECS is a family of gateway solutions that scale from small installations with less than 100 secure connections to large, high-availability, enterprise-class services supporting thousands of concurrent users. PacStar ECS designs are based on Curtiss-Wright's extensive experience developing tactical CSfC solutions. It is fully supported by Curtiss-Wright expert CSfC engineers and can be customized to meet program requirements.

PacStar IQ-Core EUDM is part of the PacStar IQ-Core Software family of products, including IQ-Core Network Communications Manager (NCM), IQ-Core Crypto Manager (CM), IQ-Core Continuous Monitoring Manager (CMM) and IQ-Core Remote Operations and Management (ROAM), used within PacStar CSfC solutions to simplify and unify configuration management, situational awareness, and real-time monitoring.

Key Features

- **Reduced Complexity**
  Replaces dozens of error-prone manual steps, saving hours of effort in provisioning time for CSfC end user devices
- **Compatibility**
  Supports COTS laptops from Dell or HP, provisioned with industry standard VPN clients from leading CSfC-compatible vendors
- **Compliance**
  Ensures laptops are provisioned, configured, and updated in accordance with CSfC capability packages
- **Security**
  Based on Green Hills Software Common Criterial EAL6+ certified security kernel for unmatched EUD security
- **Manageability**
  Integrated with PacStar IQ-Core Software which reduces system complexity and simplifies management for system and cybersecurity administrators

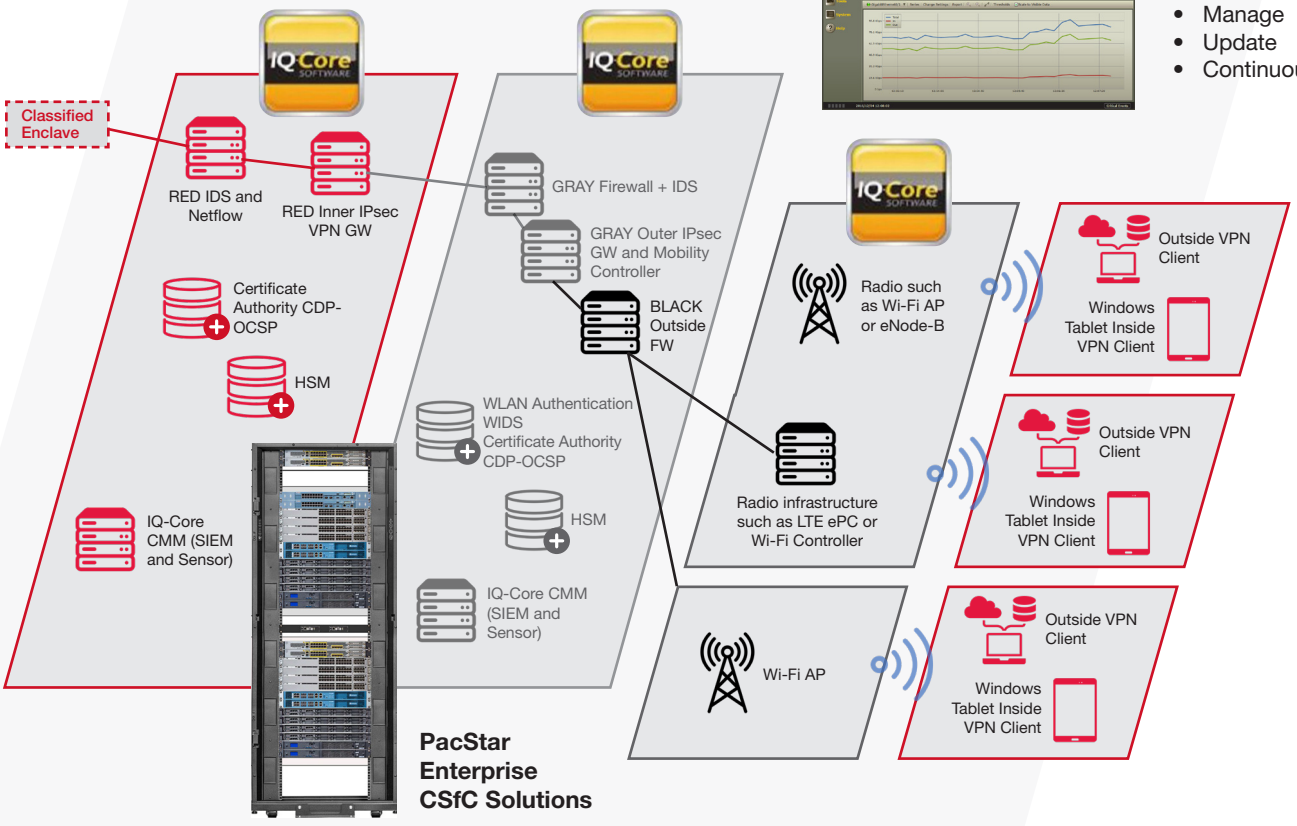
Solutions Architecture

PacStar IQ-Core EUDM manages CSfC solutions that 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. Management of both the gateway infrastructure and the SwIC EUDs is facilitated by PacStar IQ-Core EUDM.

- Faster Provisioning: PacStar IQ-Core EUDM 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 EUDM can be accomplished in as little as 7 minutes.
- Efficient Certificate Management: PacStar IQ-Core EUDM (combined with IQ-Core CM) has a vendor-neutral GUI (i.e., it supports ISC CertAgent and Red Hat Certificate Services) and tools for creating, signing, distributing, renewing and revoking certificates. Using PacStar IQ-Core EUDM, EUD certificate management is performed over-the-air.
- Automated Updates: The PacStar IQ-Core EUDM "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 combination of PacStar ECS, PacStar IQ-Core EUDM, and laptops with IGS SwIC provides an end-to-end solution that allows mobile devices to use multiple transports without additional changes to the security architecture. Transports can include terrestrial circuits, Wi-Fi, cellular, satellite, etc.

Example Logical Network for Deploying Secure EUDs with SwIC



PacStar IQ-Core® Software

- Configure
- Provision
- Manage
- Update
- Continuous Monitoring

Secure End User Devices with IGS SwIC

The foundation of the EUD security is the Secured with INTEGRITY Client (SwIC) from IGS. It is based on the Green Hills Software INTEGRITY-178B Separation Kernel, the only separation kernel certified by National Information Assurance Partnership (NIAP) to EAL6+ High Robustness, as well being certified against the U.S. Government Common Criteria Protection Profile: “Protection Profile for Separation Kernels in Environments Requiring High Robustness”.

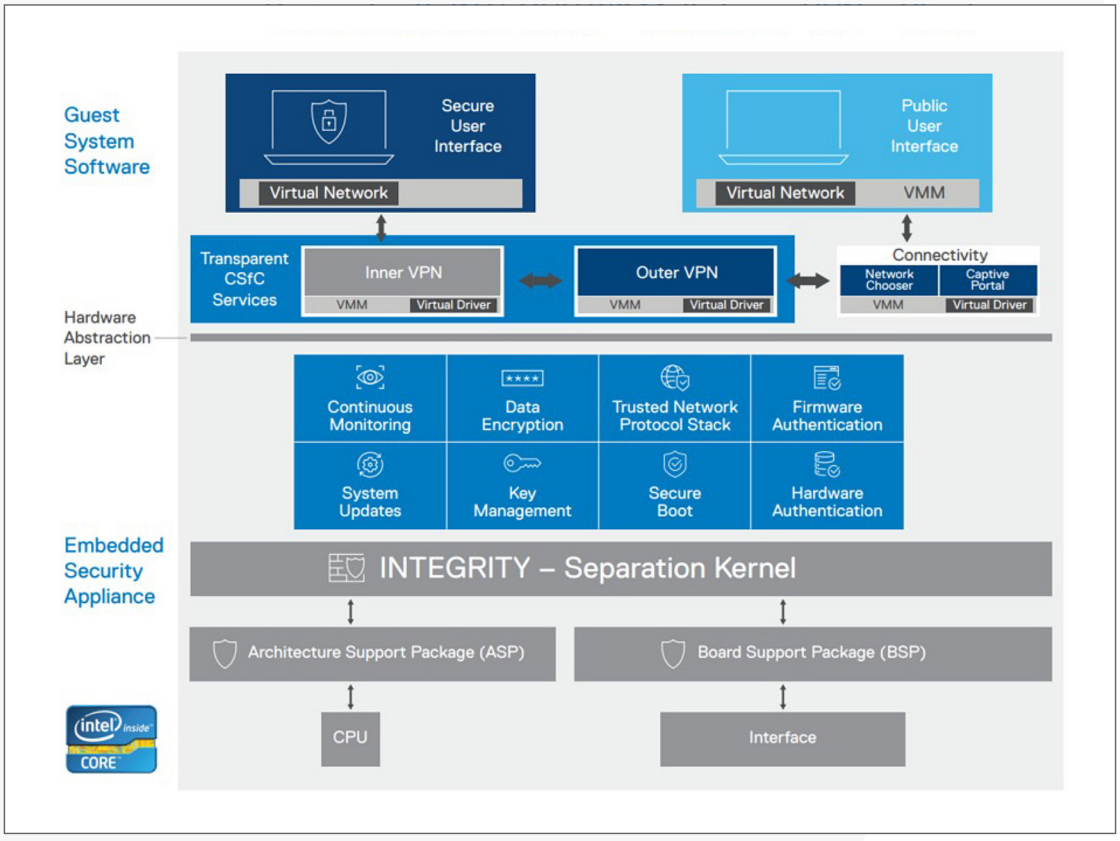
The SwIC client allows for applications to run natively on the INTEGRITY OS as well as hosting guest operating systems through virtualization. This creates a highly versatile and secure appliance that minimizes system administration and significantly reduces security risk by providing high-assurance process separation and isolation of data.

INTEGRITY implements virtualization to provide support for multiple guest operating environments. The separation kernel architecture is leveraged to provide guaranteed separation of the virtualization components as well as the guest operating system. This creates a construct that includes the Virtual Machine Manager (VMM) or hypervisor code within the same isolated virtual address space as the guest. This prevents exploitation of the VMM providing a “VM escape” and allowing a low-privilege process access to a high-privilege process. This is a significant architectural difference from all other commercial hypervisors available today.

Organizational security policy is embedded into the specified security architecture of the platform. Once integrated into the platform, the application and user environments can be managed and updated through normal configuration management processes.

The diagram below shows multiple guest OS environments isolated in their own virtual address spaces. The virtualization components (VMM) also reside within the same address space as the guest. INTEGRITY maintains the construct, communication parameters, and isolation rules of each of the processes and provides a seamless interface for users to work with.

Secured with INTEGRITY™ Multi-Layer VPN - Client



PacStar IQ-Core EUDM

Because CSfC systems require two independent encryption systems, including PKI from two different vendors or platforms, they add complexity and training burden on organizations. PacStar 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

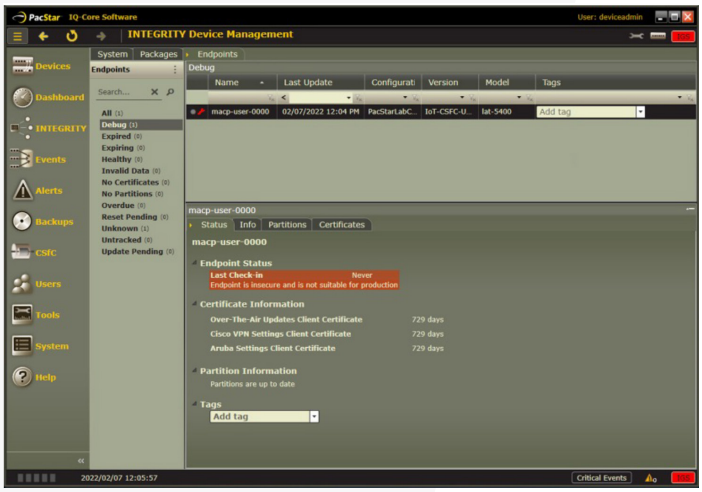
PacStar IQ-Core Software comprises a family of software editions designed to address common challenges in managing systems composed of equipment and software from multiple vendors. The editions include IQ-Core Network Communications Manager (NCM), IQ-Core Crypto Manager (CM) and IQ-Core Continuous Monitoring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

PacStar IQ-Core End User Device Manager (EUDM)

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

PacStar IQ-Core EUDM:

- Provides full lifecycle management of the system
- Provisions and manages SwIC - enabled EUDs for compliance with the NSA CSfC MACP
- Replaces dozens or hundreds of error-prone steps, per EUD, saving hours of provisioning time
  - Some organizations report 4-5 hours per EUD for provisioning w/o IQ-Core Software
  - Provisions machines in 7 minutes
- Conducts over-the-air updates including for certificate renewal, prior to certificate revocation
- Compares configurations and enforces configuration
- Collects audit logs and events



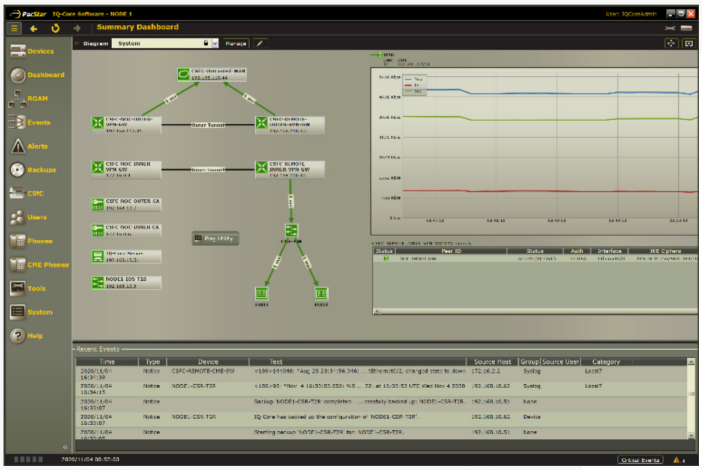
PacStar IQ-Core Crypto Manager (CM)

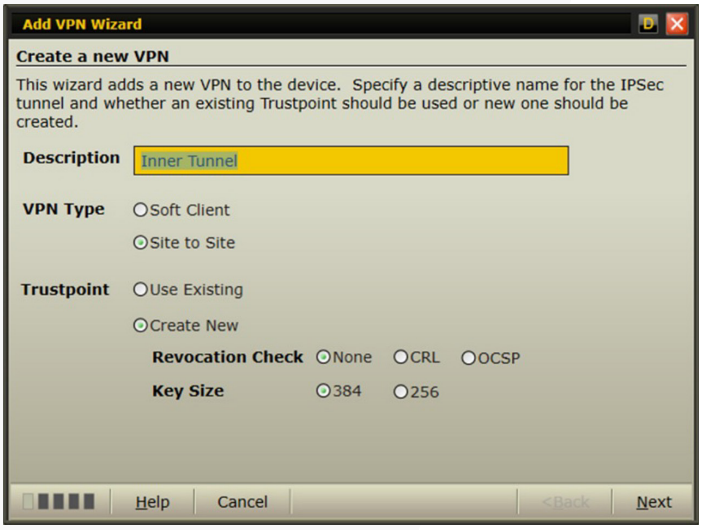
PacStar IQ-Core CM is purpose-built to manage CSfC solutions.

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.



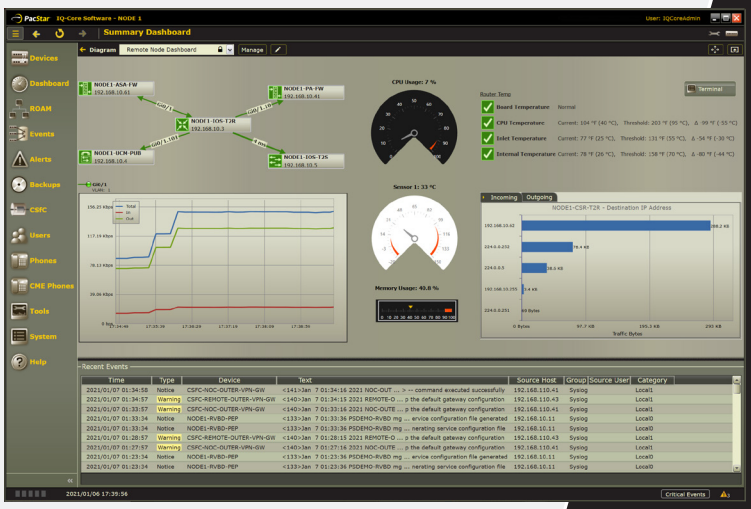


PacStar IQ-Core Network Communications Manager (NCM)

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 role-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 products are covered by multiple patents. Additional patent(s) pending.

PacStar IQ-Core EUDM