



IQ-Core Crypto Manager (CM)

Unified Network Communications Management

To enable mobility for warfighting, the National Security Agency (NSA) established a program (with a set of guidelines) called “Commercial Solutions for Classified” (CSfC). This program enables U.S. DoD and federal organizations to transmit classified information, up to Top Secret, using commercial-grade encryption solutions, eliminating the need for expensive, difficult-to-use classified equipment.

CSfC enables access to classified information using inexpensive, commercial technologies, providing benefits such as:

- Enabling entirely new classes of wireless access to classified networks for warfighting
- Enabling U.S. coalition partners to access classified information without taking possession of controlled cryptographic items (CCI)
- Significantly reducing equipment costs and simplifying key management
- Simplifying equipment handling and security procedures

CSfC guidelines provide configuration options that allow classified data to be transmitted using two layers of Commercial Off-the-Shelf (COTS) encryption products. Previously, the only way to transmit classified data was by using expensive, controlled, military-grade encryption devices such as SECNET-54s and KG-250s.

However, these systems are complex to set up, configure, secure, and maintain because they include many complex components from multiple vendors or platforms.

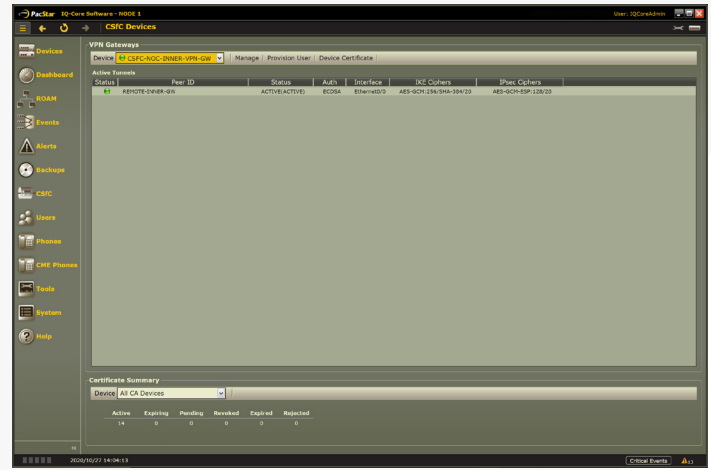
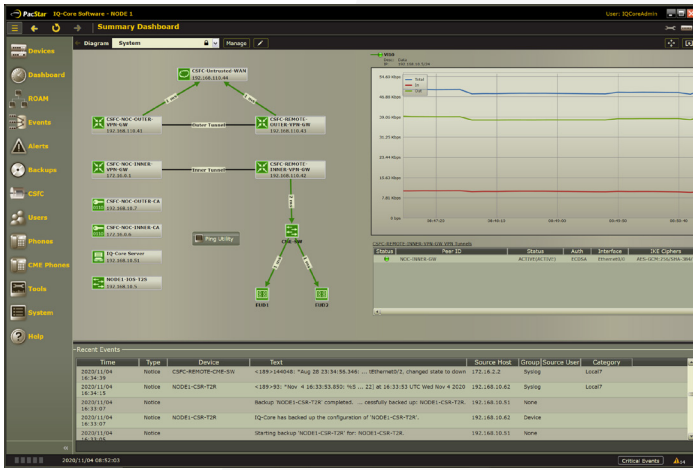
IQ-Core® CM overcomes the added complexity and training burden imposed by the two layers of encryption by simplifying the setup, configuration, and management of the underlying equipment used in CSfC solutions.

Key Features

- An intuitive user interface through wizards, making CSfC set-up and operation quick, easy-to-learn & recall
- Reduces configuration errors by assisting organizations in maintaining uptime and compliance with stringent CSfC requirements
- Simplifies troubleshooting with integrated tools for both entry-level and advanced network administrators - with CSfC-optimized tools link status, coordination of device time, monitoring of certificates, and more
- Saves time by automating complex, time consuming, and error-prone tasks, with powerful wizards common user interfaces across hardware, software, and PKI components
- Provides cyber situational awareness (SA) by securing and consolidating alerting information at the edge while also working with enterprise SIEM. Provides enhanced CSfC SA at the core and edge of the network with extensive real-time status of crypto tunnels, certificate expiration alerts, & connection auditing.
- Facilitates remote and distributed management through the ability to perform CSfC-related management tasks from anywhere in the world
- Streamlines innovation by interoperating with a broad range of tactical and enterprise CSfC-certified communications hardware and systems, simplifying upgrades and adoption of new COTS technologies at the edge

Certified and included on the DoDIN Approved Products List (APL)

IQ-Core CM screen shots

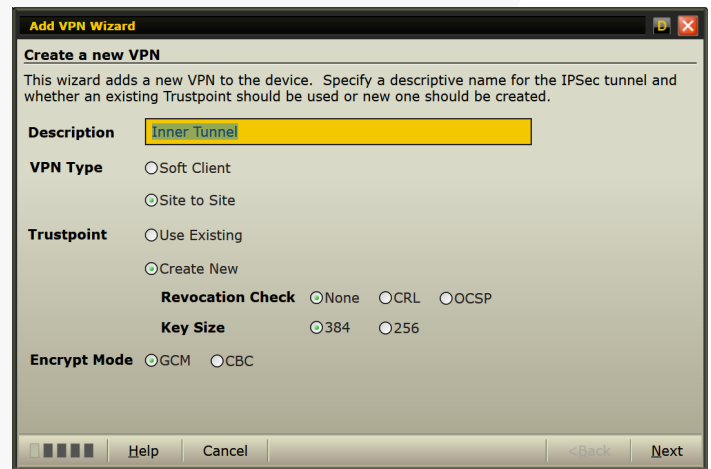


Customizable dashboards

- Monitor the status of CSfC components from multiple vendors, from a single view
- View real-time status of VPN tunnels including WAN and EUDs
- Provide system-at-a-glance status including hardware, software, and VMs

CSfC devices view

- Track CSfC device status and tunnels, including IKEv1 and IKEv2
- Certificate authority status at a glance, including active certs summary
- Easy navigation to key CSfC capabilities



Certificate authority management

- Create and sign certificates, revoke certificates, create CRLs
- Track and alert on certificate expirations
- Consistent UI regardless of CA vendor -- minimizes training

Add VPN wizard -- VPN setup

- Automates creation of VPNs on VPN gateways
- Provides simple, step-by-step instructions
- Applies VPN settings to VPN gateways, consistent with CSfC requirements

IQ-Core Crypto Manager

IQ-Core CM screen shots



Add VPN wizard -- certificates

- Generates public/private key pairs on VPN gateways -- ensures CSfC-compliant settings
- Creates certificate signing requests and transmits to certificate authority
- Loads signed certificates onto VPN gateways

Feature summary

IQ-Core CM adds the following CSfC-specific functionality:

- VPN set-up wizards
- VPN configuration at a glance
- VPN monitoring/troubleshooting
- Certificate management

VPN setup wizards

IQ-Core Software VPN setup and certificate generation wizards reduce the complexity of providing the correct information to CSfC devices by providing step-by-step guidance, insulating lightly-trained users from dealing with the command line interfaces and multiple UIs across the underlying devices.

VPN configuration at a glance

For Cisco devices, IQ-Core CM displays the configuration settings in an IPsec gateway, incorporating information about trustpoints, IKE Proposals and IPsec parameters.

IQ-Core Crypto Manager

Event management

- Collects events from CSfC components in Syslog and WMI formats. Provides northbound log forwarding and local storage.
- Provides comprehensive searching capabilities
- Assists in CSfC continuous monitoring requirements

VPN monitoring/troubleshooting

IQ-Core CM VPN monitoring capabilities include the ability to display, in real time, the connection status of one or more VPN endpoints connected to the device under management. Within the status is an indicator of the active authentication and bulk encryption settings in use.

Certificate management

IQ-Core CM automates the process of managing device certificates, a process that is error-prone and requires extensive training. Reducing the opportunity for errors in this process improves communications uptime and allows security administrators to focus on more important tasks. IQ-Core Software capabilities related to CSfC certificates include:

- Generation of certificate signing requests
- Display of certificate details and expiration dates, including expiration alerts
- Encrypted transmission of certificate signing requests
- Management of the signing process at either the deployed systems or at the NOC
- Management/monitoring of certificate authorities

Feature summary

Available now

IQ-Core CM supports the capabilities for CSfC components including:

- Aruba Mobility Controllers
- Cisco IOS and IOS-XE -based IPsec gateways
- Cisco ASA 5000-Series and ASAv firewalls
- Information Security Corp CertAgent
- Juniper vSRX firewalls
- Microsoft Active Directory Certificate Services

Red Hat certificate services

The NSA CSfC program office has specified that IQ-Core CM may be included in any CSfC solution without further CSfC certification. IQ-Core Software may be used for the management of red, gray, and black network equipment when individual copies are installed and configured in each network in accordance with requirements for other management tools.

IQ-Core Network Communications Manager (NCM) and CSfC

IQ-Core CM is built on top of IQ-Core NCM, which contains extensive device and network management capabilities that streamline CSfC management. These capabilities can be used to meet many solution administration requirements and procedures. IQ-Core NCM simplifies set-up, monitoring, and troubleshooting device configuration, manages logs and alerts to support continuous monitoring, and more. See the IQ-Core NCM datasheet for more information.

IQ-Core Crypto Manager