



IQ-Core[®] CMM

Continuous Monitoring Manager (CMM) for Commercial Solutions for Classified

Implementation of Continuous Monitoring (CM) is a requirement of the NSA Commercial Solutions for Classified (CSfC) program, that must be met prior to approval and deployment of CSfC solutions.

In CSfC, CM is implemented as part of a holistic, risk management and defense-in-depth information security strategy integrated into CSfC architectures. Organizations designing CSfC solutions and implementing CM capabilities must use information gathered from CM capabilities to take appropriate risk mitigation actions regarding the operation of CSfC systems.

The NSA Continuous Monitoring Annex to CSfC capability packages provides guidance for the collection and analysis of network and security data to enable CM within a deployed CSfC solution. In CSfC's data-in-transit multi-layered approach to encryption, failure of one or more components may result in observable network behavior that significantly deviates from established baselines.

IQ-Core Continuous Monitoring Manager offers the fastest and least expensive method to meet requirements for CSfC infrastructure. IQ-Core CMM includes security sensors, data collection and security information, and event management (SIEM) technologies required to meet CSfC requirements. IQ-Core CMM, like all Curtiss-Wright CSfC solutions, is delivered to customers as a complete solution. The system is configured, locked down, and tested to function in accordance with CSfC capability packages and annexes.

Key Features

- **Reduced Cost**
Built on industry-leading commercial networking and cybersecurity technology, and pre-configured into a turnkey solution, which reduces training and support costs
- **Compatibility**
Demonstrated interoperability with many of the most popular CSfC components, speeding implementation and deployment
- **Compliance**
Configured and tested by Curtiss-Wright to ensure compliance with CSfC Continuous Monitoring Annex requirements for infrastructure
- **Security**
Pre-configured to meet DISA STIGs and SRGs to ensure a strong security posture
- **Manageability**
Integrated with IQ-Core Software, reducing system complexity and simplifying

IQ-Core CMM and IQ-Core Software

IQ-Core CMM offers industry leading technology with high-performance data collection and search, including an embedded SIEM capability (with collection of syslog and NetFlow information), and a dedicated network sensor for network traffic capture.

Key IQ-Core CMM technology benefits include:

- Provide high performance SIEM and search
- Are turnkey, configured and tested by Curtiss-Wright to meet CSfC requirements, eliminating substantial expense and time otherwise required to tailor the system
- Provide a cost-effective solution with predictable expense, to system throughput / usage
- SIEM, which is well-supported in defense and federal markets, with rapidly increasing adoption
- Meet stringent DOD and federal security requirements

IQ-Core CMM integrates with the family of IQ-Core Software editions designed to address common challenges in managing systems consisting of equipment and software from multiple vendors. They work together providing advanced, unified management of Curtiss-Wright CSfC Solutions.

IQ-Core Software Integration

IQ-Core CMM works with the family of IQ-Core Software editions by providing integrated dashboards, displaying key information, status, and alerts generated by the embedded SIEM engine.

IQ-Core CMM provides further alerts, integrated into IQ-Core Software's event and alert system, through APIs.

This integration results in an IQ-Core Software solution that:

- **Provides an intuitive user interface:** 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
- **Facilitates remote and distributed management:** Ability to monitor, change device configurations and troubleshoot from anywhere in the world



IQ-Core CMM

IQ-Core CMM Use Cases

Integrated into Curtiss-Wright Tactical Solutions

- Increase security and visibility for new and existing communications solutions
- Ensure compliance with NSA CSfC requirements
- Runs on dedicated hardware for high performance
- Available in virtualized configuration sharing compute resources, for reduction in SWaP

Available in Curtiss-Wright Enterprise CSfC Solutions

- Runs on enterprise class, 19' rack mount hardware
- Scalable Options:
 - Small installation ≤ 100 concurrent connections
 - Large installation (with High Availability) ≤ 5000 concurrent connections

Turn-Key Implementation and Experienced Technical Support

Example Two-Enclave IQ-Core CMM in Tactical Hardware



Solutions Architecture

IQ-Core CMM, combined with Curtiss-Wright technical expertise in tactical communications, and integration, testing, and certification experience, delivers continuous monitoring solutions for fixed installations, using enterprise COTS rack-mount equipment, for tactical applications, using tactical hardware with or without virtualization

IQ-Core CMM includes the following capabilities:

- Monitors the required network/infrastructure monitoring points.
- Collects monitoring data:
 - Includes logs/alerts collected from infrastructure devices (switches, firewalls, CAs, etc.) and encryption components (VPN gateways, WLAN controllers) via syslog

IQ-Core CMM

Curtiss-Wright Enterprise CSfC Solutions (Mobile Access Gateway with High Availability)

• Cisco Firepower

- Aruba VPN Controller
- Cisco Data Switch
- Cisco Management Switch
- Palo Alto TFW
- Management Server
- Network HSM

• NTP Servers

- Cisco VPN Controller
- Cisco Data Switch
- Cisco Management Switch
- Palo Alto IDS
- Management Server
- Network HSM



- Includes collecting NetFlow data from red and gray firewalls
- Includes collecting packet capture from the monitored network segments.
- Analyzes data for unusual / prohibited behaviors and traffic
- Provides dashboards and alerts to security administrators
- Stores and manages logs

IQ-Core CMM supports infrastructure requirements for all NSA CSfC Capability packages, when integrated with Curtiss-Wright CSfC solutions.

In Curtiss-Wright CSfC solutions, IQ-Core CMM collects and monitors network and cybersecurity information at required locations in a CSfC network, in accordance with the CSfC Continuous Monitoring annex requirements per the table below, for infrastructure.

Example Logical Network for IQ-Core CMM in a CSfC Multi-site Connectivity Capability Package

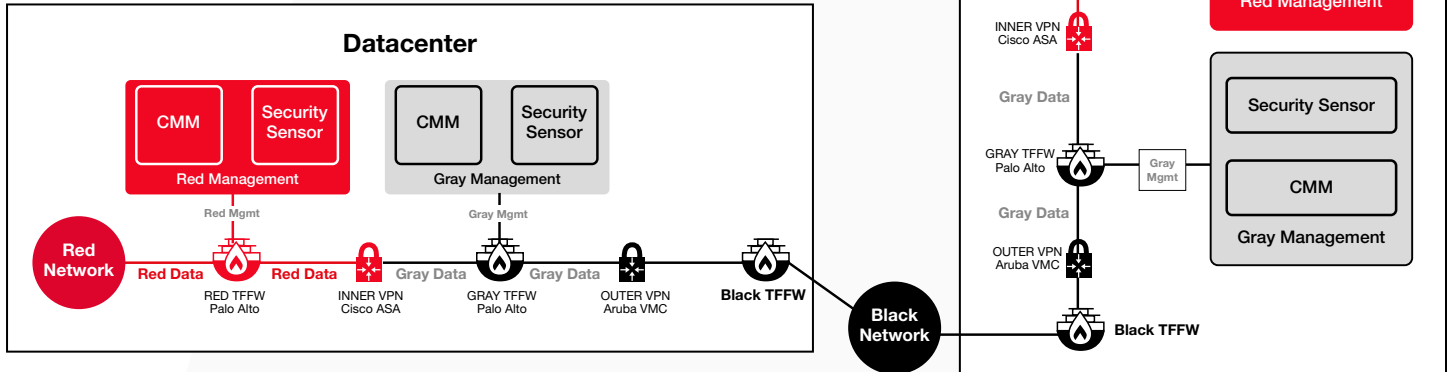


Table 1: Required MP Deployments for CSfC Solutions

CP	Required	Choose One MP in Black or Gray Networks	Choose one MP in Red Network
MA	MP6, MP7, MP8 and *WIDS	MP1, MP2, MP3	MP4, MP5
WLAN	WIDS, MP6, MP7 and MP8	MP2, MP3	MP4, MP5
MSC	MP6 and MP7	MP1, MP2, MP3	MP4, MP5

Monitoring Point 3

- Monitoring point 3 resides in the data network between the gray firewall and inner encryption component.
- At this location, IQ-Core CMM collects packet capture data from the data network.

Monitoring Point 4

- Monitoring point 4 resides in the data network, between the inner encryption component and inner firewall.
- At this location, IQ-Core CMM collects packet capture data from the data network.

Monitoring Point 6

- Monitoring point 6 resides in the gray management network.
- At this location, IQ-Core CMM collects the following information from the management network: Syslog and NetFlow from the gray firewall, Syslog from Aruba Clearpass (WLAN CP only), packet capture.

Monitoring Point 7

- Monitoring point 7 resides in the red management network.
- At this location, IQ-Core CMM collects the following information from the management network: Syslog and NetFlow from inner encryption component and firewall, packet capture.

WIDS

- For Curtiss-Wright WLAN CP-based solutions, WIDS is supported so long as the WIDS AP is connected to and managed by the gray network.
- For tactical deployments, WIDS is optional, per the tactical appendix to the Continuous Monitoring Annex (and the WLAN CP).

IQ-Core CMM