Viakoo Device Certificate Manager

Zero Trust Enterprise IoT Device Certificate Management

Thwart Ransomware Attacks Originating Through IoT Devices with Automated Provisioning and Management of Certificates

Ensuring every device on the network has authentic and current certificates is a critical action toward protecting against cyber attacks. The process of provisioning and maintaining certificates on thousands of devices from multiple vendors has been a complex and impossible manual task. With Viakoo Device Certificate Manager the process is automated across IoT devices, at enterprise scale. From a single user interface certificates can be provisioned, status confirmed, refreshed, and revoked at will as needed.

- Extend zero trust coverage to IoT devices with 802.1x/TLS/OPC-UA certificates
- Ease the burden of provisioning and managing certificates at enterprise scale on IoT devices
- Repatriate IoT devices into production as fully documented network citizens
- Automate compliance and governance audits for IoT devices
- Enterprise-wide automated full life cycle management of certificates, including 802.1x, TLS/LLS, OPC-UA and others
- Support both Tightly Coupled and Loosely Coupled IoT devices with equal confidence
- Certificate integrity through built-in chain-of-custody security

Achieve Zero Trust Security with Certificates for all IoT Devices

Viakoo Device Certificate Manager manages all IoT device certificate status, including confirming certificate presence, expiration date, and authenticity. DCM automates initial provisioning of certificates and maintains an audit log per device of certificate history for compliance and governance. DCM uses a chain-of-trust methodology to ensure certificate security from the correct Certificate Authority to each IoT device.

DCM Manages IoT Device Certificates

- 802.1x
- TLS/LLS
- OPC-UA

Data to Insight to Action

Viakoo DCM gives you detailed information about your IoT devices, their certificate status, and automated action to maintain them.

Always Be Compliant

Whether to meet internal governance or to successfully pass external audits, Viakoo DCM guides your team to always be in compliance.

Secure Chain-of-Custody

Viakoo DCM incorporates an end to end process to ensure device certificates cannot be modified or compromised.

Comprehensive To Reduce Attack Surface

Whatever types of devices are in the enterprise, from printers to cameras to sensors, DCM manages the variety of certificates to ensure known-good status of all network citizens. DCM gives you the power to perform bulk updating based on Device Type, Model, or Certificate Type. DCM is a module of the Viakoo Action Platform™ that together deliver full remediation and repatriation of IoT devices to complete an enterprise IoT security solution.

Reduce Your Cyber Risk

- Flexibility to use 3rd party or internal Certificate Authority
- Automate identification of missing or expired certificates
- Monitor job status to easily see or modify certificate operations
- Eliminates need to log into multiple dashboards
- Automate certificate compliance reporting

VIAKOO ACTION PLATFORM™ SUITE

The complete Viakoo Action Platform Suite includes:

Device Firmware Manager (DFM)
Device Certificate Manager (DCM)
Device Password Manager (DPM)

Enabling the enterprise with the Viakoo Action Platform Suite

The Viakoo Action Platform with DFM, DCM, and DPM is a complete enterprise IoT device security solution solving the problem of managing fleets of 100,000s of IoT devices affordably. Delivered as a SaaS offering, the solution ensures all devices are inventoried, in compliance with internal policy, and are continuously remediated and repatriated as full, secure network citizens. This

scalable, automated solution reduces an organization's risk, saves time and cost while delivering on IoT device ROI. The flexible and modular solution allows you to start small and grow over time while delivering value at each step.

VIAKOO ACTION PLATFORM™ MODULES

Device Firmware Manager

Security patches are crucial for IoT device security. Security patches are made through IoT firmware upgrades and must be implemented continuously as they become available.

Device Firmware Manager automates the process of firmware updates on IoT devices, at scale across the enterprise. DFM provides compliance reporting complete with a history of changes for audit purposes. A secure "chain-of-trust" ensures only valid and functional firmware is deployed, and complete automation allows for updates of thousands of devices wherever they live. Get the Device Firmware Manager data sheet.

Device Password Manager

Device Password Manager automates the process of setting, maintaining, and managing IoT device passwords, at scale. DPM automates verification of password and password policy management for thousands of IoT devices from a wide variety of vendors, providing password status, automated checking, and an audit trail for governance. Get the Device Password Manager data sheet.

Device Certificate Manager

Zero trust depends on authentication generally achieved through the use of Certificates. Device Certificate Manager enables zero trust by automating the process of provisioning, refreshing, and revoking IoT device certificates such as 802.1x, TLS/SSL, OPC-UA and others. DCM provides detailed information on both managed and unmanaged IoT devices, their certificate status, and automates actions to maintain them. A chain-of-custody process in incorporated to ensure device certificates cannot be modified or compromised.

Master the security of your cyber-physical systems with the Viakoo Action Platform.