Datasheet

Keyfactor
Command for IoT

Protect and manage IoT identities at scale.

Establish and maintain trust in your IoT products. Keyfactor Command for IoT is an end-to-end IoT identity management and automation platform for a device's entire lifecycle.

Whether building medical devices, vehicles, smart home devices, or any other connected device, tight budgets, hardware constraints, and complex IoT supply chains make it hard to build strong security into your products at scale. But when safety and security are at stake — it must happen.

Machine identities in the form of digital certificates serve as the backbone of digital trust in IoT devices. However, outdated tools and gaps in visibility leave many teams exposed to security risks caused by untracked and insecure digital certificates and certificate authorities.

Keyfactor Command for IoT delivers 100% visibility across all a business's certificate authorities (CA) and digital certificates. Features like role-based security controls and automated workflows simplify operations and ensure that every identity is trusted, valid, and compliant, no matter where they were issued from. Additionally, a flexible architecture allows Command for IoT to be deployed on a private cloud or data center, directly from the Azure marketplace, hosted by Keyfactor, or as a SaaS model.

Establish trust

Security is no longer optional for IoT devices. As part of a connected network, IoT devices need to communicate with other devices, receive updates, and, when the time comes, have their permissions revoked as part of an end-of-life process. Certificates are at the core of providing IoT devices with unique and trusted identities.

Use Cases

Issue, provision, renew, and revoke certificates and keys throughout the device lifecycle from one platform.

Monitor all certificates from all CAs, public and private, in a single dashboard.

Decommission devices at scale or respond to incidents with simple one-click revocation, whether for one certificate or millions.

Key Benefits

Streamline manufacturing by automatically registering and provisioning device identities in large volumes.

Quickly identify and remediate risks with a simple search-and-click engine.

Organize certificate inventories into manageable collections with custom metadata tags.

Simplify audits and meet compliance requirements with real-time visibility of all certificates and easy-to-generate reports.

Scale on demand, without limits or per-certificate fees with a flexible PKI architecture.

Keyfactor Command for IoT provisions identities at scale, whether directly in a factory or remotely to already deployed devices when identities need to be updated. Additionally, with flexible architecture options, the PKI solution can be deployed locally, in the cloud, hosted, or as a service to match a manufacturer's current needs and capabilities.

Maintain trust

Issuing identities is just the first step. Certificates will need to be renewed and possibly revoked throughout the device's lifetime. However, monitoring the status of possibly millions of devices manually with a spreadsheet is nearly impossible.

With Keyfactor Command for IoT's built-in dashboards and advanced tags and searching features, finding soon-to-be expiring certificates is simplified. Taken one step further, automated workflows can automatically renew certificates, or reports can be generated for administrators to be able to see which devices or groups of devices will soon need attention.

Enable Crypto-Agility

Avoid costly product warranty recalls related to cybersecurity patches by ensuring that device identities can be updated remotely, whether online or offline. In the event that a root of trust needs to be replaced to brownfield devices, it's critical to have a scalable and trustworthy process for updating device identities remotely.

Keyfactor Command for IoT provides full lifecycle automation capabilities for manufacturers and operators to be able to keep device cryptographic material up to the latest standards, including preparing for post-quantum resilience.

Key Features

Integrate with external SIEM or ITSM tools for automated workflows that enable renewal alerts, scheduled compliance reports, and more.

Use a lightweight C POSIX, Android, or Java agent to enable on-device identity lifecycle management and automation.

Easily integrate with third-party CAs, cloud services, and IoT platforms such as Azure IoT Hub.

Automatically renew and provision certificates to remote devices anywhere, from any public or private CA.

Combine Keyfactor Command for IoT with EJBCA Enterprise to issue IoT identities at a massive scale from a trusted PKI platform.

Deploy in your own data center or cloud, directly from the Azure marketplace, as a service from Keyfactor, or managed in a private PKI cloud from Keyfactor.

Monitor, manage, and, if necessary, swap out roots of trust.

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

To get started with Command for IoT, contact us at sales@keyfactor.com or via phone at +1 (216)-785-2946.