Password Rotation for IoT devices

IAM to efficiently change 10,000’s of passwords for hackable IoT devices

Use case

Cyber criminals and attackers are increasingly exploiting weaknesses in IoT device identities. Manufacturer set default passwords which remain unchanged. These unchanged passwords are proving are to be the Holy Grail for hackers. According to Verizon DBIR, 63% of security incidents were related to weak credentials and this attack vector has proven responsible for the recent Mirai and BrickerBot attacks.

IAM consists of tools and practices that keep an organization safe from accidental or deliberate misuse of access. An IAM offers a secure, streamlined way to authorize and monitor all privileged users for all relevant systems:
Situation

Regularly changing the current passwords with new ones is an resource- and time-consuming but necessary way to improve security. That’s why organizations demand their staff to change passwords based on a recurring event (e.g. every two weeks).

The main idea behind password rotation can be summarized as “a rolling stone gathers no moss.” All too often, companies and manufactures are leveraging the same password in thousands of devices. When given the choice, most people would rather have their logins be a simple as possible. They’ve already memorized their “secure” work password, so why not use it on all IoT Devices?

The issue with this attitude is that if one devices is compromised, then that puts the business at significant risk. Default device passwords can often been found on the web. Once it is known, the risk for all devices with unchanged passwords is high.

Solution

Nokia NetGuard Identity Access Manager automates password rotations to ensure compliance with corporate password aging policies. IAM achieves OPEX savings by management workflows automation as well as password rotations with a centralized access management for the whole eco-system. IAM supports configurable automatic password changes after each use, based on regular time intervals — or both.

Benefits

• Meet compliance requirements (HIPAA, GDPR, PCI-DSS, NIST, SOX, NERC CIP ...)
• Optimize access security and reduce risk exposure by maintaining control over shared accounts, service accounts, default passwords, etc.
• Receive alerts in real-time and analyze incidents.
• Opex Savings with rapid deployment into existing environments and automated pw-changes

NetGuard IAM is designed for critical communication networks and incorporates Nokia’s 30+ years of experience in helping utilities build operational communications networks.

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2018 Nokia
Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1805025090EN (May) CID205171