BOSCH
Invented for life

Device management: how to master complexity in IoT deployments

A guide to successful IoT device life-cycle management

White paper | October 2021

Contents

1. Introduction 3

2. Complexity of enterprise IoT deployment 5

2.1. Diversity of devices and software 5

2.2. Scale 6

2.3. Security 6

3. IoT device life-cycle management 7

3.1. End-to-end security 7

3.2. Precommissioning 8

3.3. Commissioning 8

3.4. Operations 8

3.5. Decommissioning 13

4. Conclusion 13

1. Introduction

The Internet of Things (IoT) has the power to dramatically increase the efficiency of businesses in numerous domains and to create completely new business models. Through real-time bilateral communication with the connected smart devices you will not only receive valuable data collected by the devices but will also be able to fulfill their maintenance and management automatically and remotely. Thus to successfully deploy an IoT solution for an enterprise, it is crucial to consider the foundation of any IoT solution: device management.

Enterprises can expect a complex IoT device landscape with heterogeneous devices that need to be managed throughout the whole device life cycle. IoT-related scenarios are getting more complex and require the execution of more sophisticated commands. Similar to the operating systems of our desktop computers, smartphones, and tablets, IoT gateways and edge devices need frequent care in the form of software updates or changes to configurations in order to improve security, deploy new applications, or extend features of existing applications. This white paper will show why robust device management is key for a successful enterprise IoT strategy.

Bosch ConnectedWorld Blog

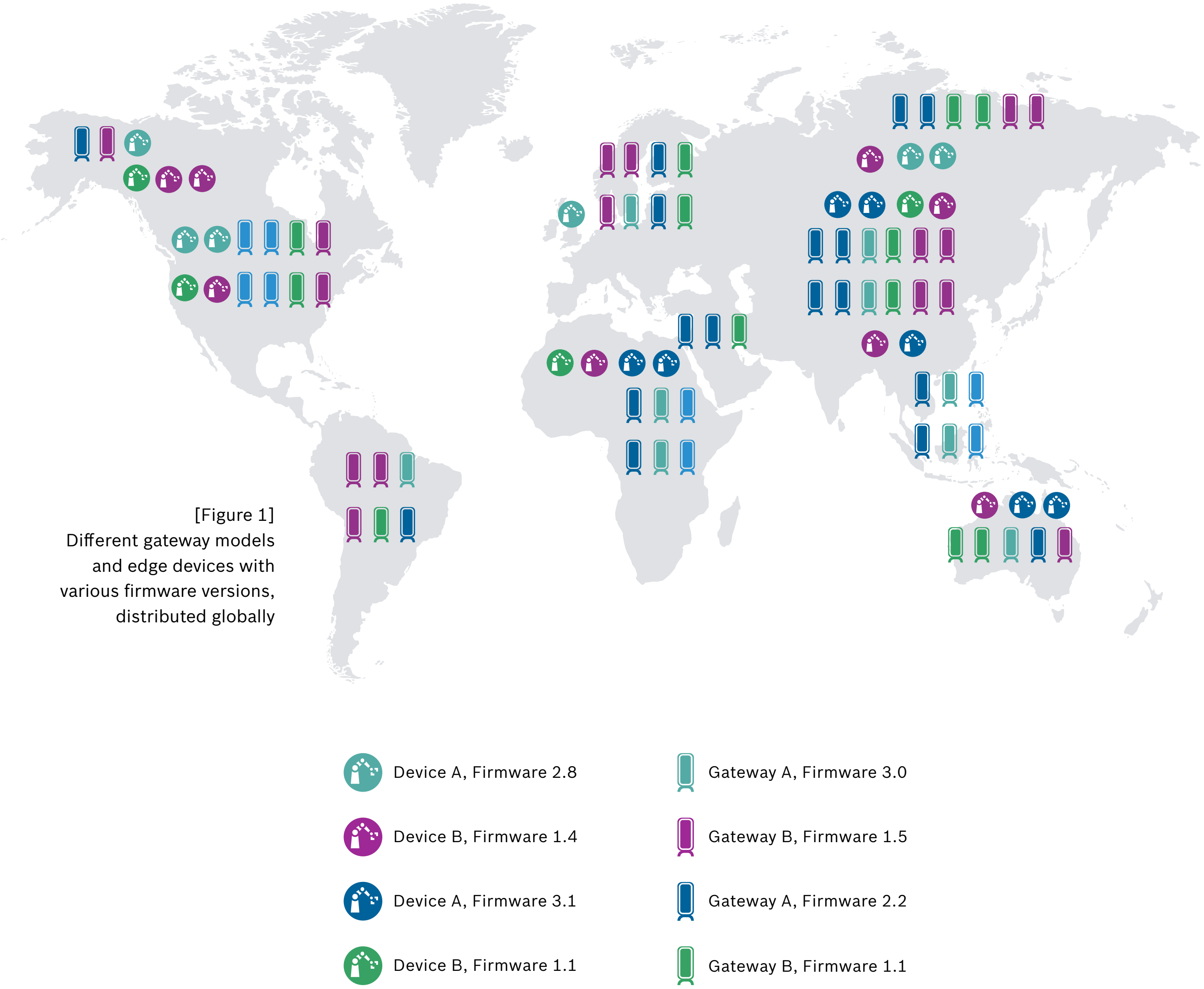
8 IoT device management use cases

Device management: the key to future-proof IoT deployments

Read the report

Bosch IoT Suite rated as leading IoT platform for device management

An IoT solution scenario generally includes connecting devices. Web-enabled devices can be connected directly, while those that are not web-enabled are connected through a gateway. The heterogeneity and diversity of constantly evolving devices is a defining factor of an enterprise IoT architecture.



[Figure 1]
Different gateway models and edge devices with various firmware versions, distributed globally

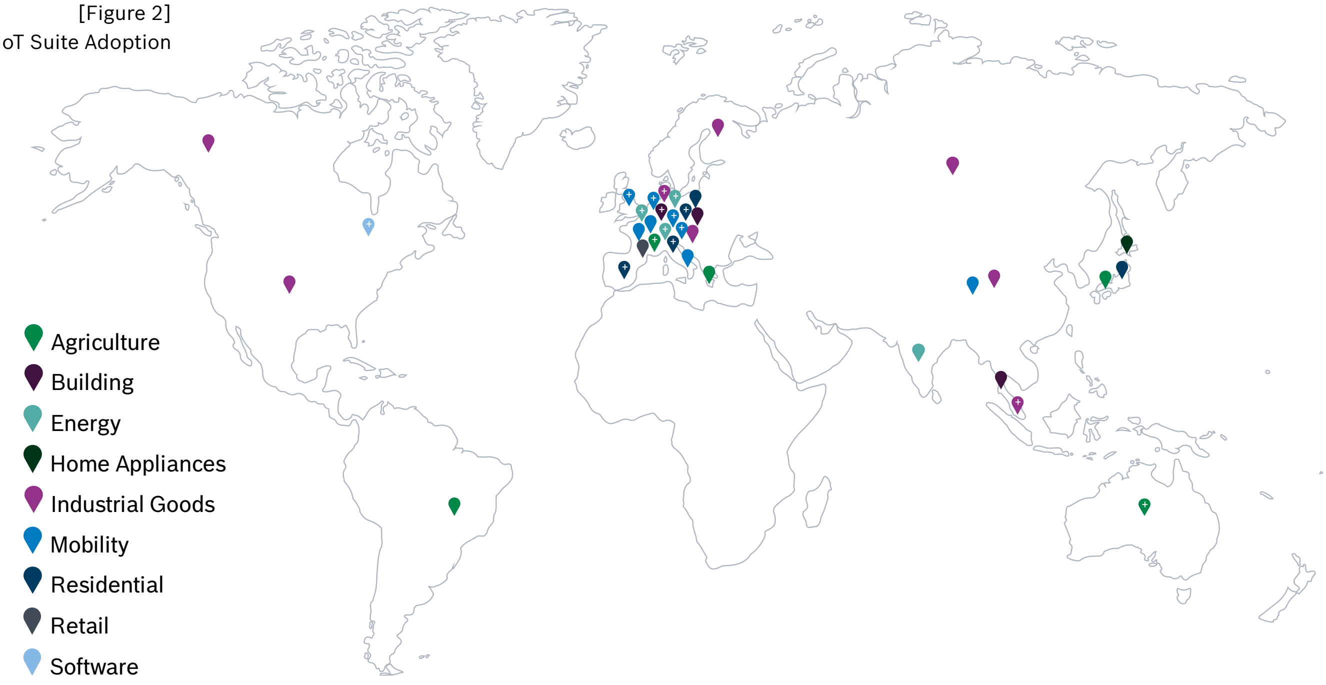
2. Complexity of enterprise IoT deployment

2.1. Diversity of devices and software

During the initial prototyping stage, the key goal is to show how devices can be connected and what values can be gained from analyzing the device data. Companies that deploy at this early stage without considering a feature-rich device management solution will soon find themselves unable to handle the growing number of device and software configurations. As the company's IoT initiative expands, its IoT solution will be forced to include a varied mix of devices and connection mechanisms. With diverse and distributed devices, the operations team will also have to deal with multiple firmware versions.

Recently, there has also been a shift toward performing more processing and computation at the edge as bigger edge devices are able to handle more complex commands. The software for this needs to be constantly updated if it is to extract the maximum value from the analytics, and the operations team will need a central tool to enable efficient remote maintenance. Providing a service that allows all the different parts of the solution to use a common device management platform unlocks operational efficiency and shortens the time to market significantly.

[Figure 2]
Bosch IoT Suite Adoption



Did you know? More than 15 million devices worldwide are already connected via Bosch's IoT platform.

2.2. Scale

Many IoT projects start with a proof of concept, and are often followed by a pilot with a limited number of users and devices. However, as more and more devices have to be integrated, the company needs an application or API that allows it to easily manage, monitor, and secure the rising number of diverse, globally distributed connected devices. In short, it has to find a device management solution that can scale from day one to the various deployment scenarios. A good piece of advice here is to think big but start small.

2.3. Security

Security is one of most obvious reasons why a device management platform is required even for small-scale deployments. Governments are introducing legislation that requires all IoT products to be patchable and to meet the latest industry security standards. With this in mind, any IoT solution should be designed with security as the fundamental requirement. IoT devices are often constrained due to cost factors, which can limit their security capabilities; however, even constrained IoT devices must have the ability to update their firmware and software due to security changes and bug fixes. You can’t afford to skimp on security.

3. IoT device life-cycle management

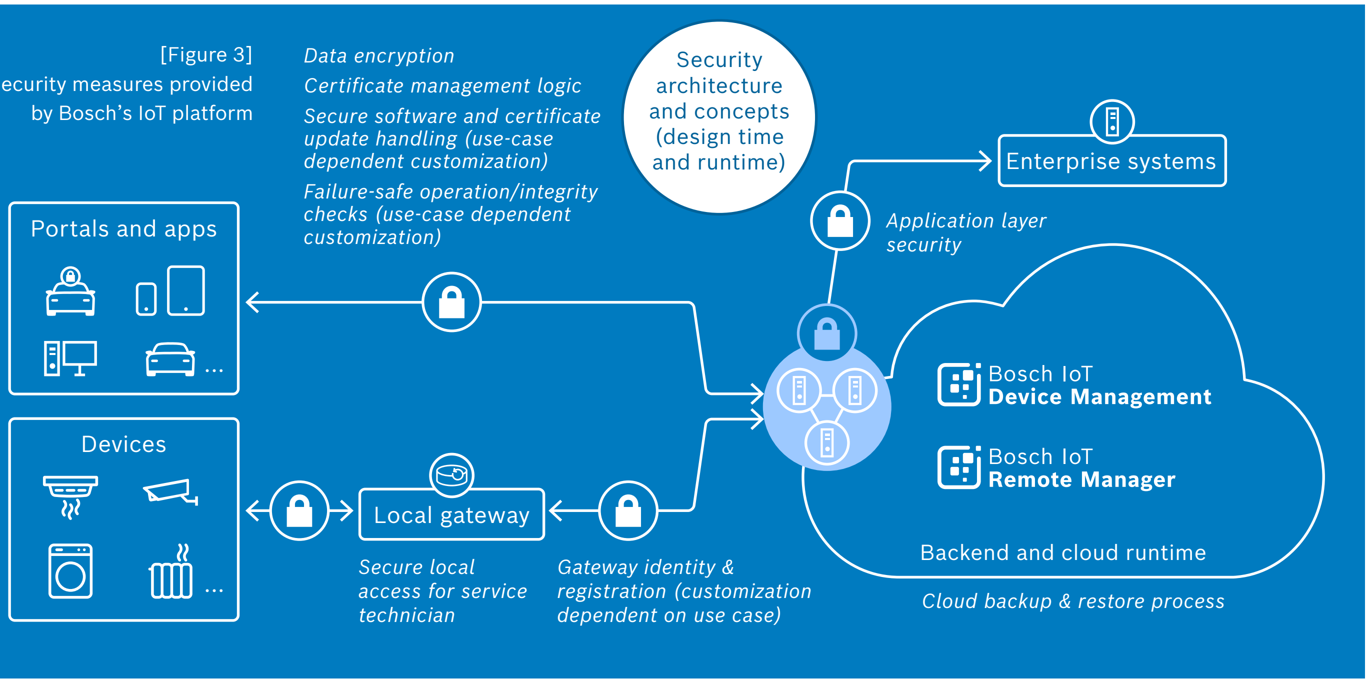
As enterprise IoT systems are expected to last many years, it is critical to design and plan for the whole life cycle of devices and applications.

This life cycle includes security, precommissioning, commissioning, operations, and decommissioning. Managing the IoT life cycle presents a high level of complexity and requires a wide range of capabilities. We aim to highlight some general components of the IoT device life cycle here; however, details also depend on the type of device management protocol used.

3.1. End-to-end security

Device authentication is especially important when establishing secured communication links. IoT devices should be authenticated using device-specific security credentials. This then enables the operations team to identify and block or disconnect devices deemed to be a threat. One way to authenticate the devices is to supply device-specific private keys and the device's corresponding digital certificates during production (e.g. X.509) and provide regular field updates of those certificates. The certificates enable backend access control based on well-established and standardized validation mechanisms such as mutually authenticated TLS, which ensures encryption for all types of connectivity. A device management solution should also be able to revoke certificates if needed.

[Figure 3]
Security measures provided by Bosch's IoT platform


Data encryption
Certificate management logic
Secure software and certificate update handling (use-case dependent customization)
Failure-safe operation/integrity checks (use-case dependent customization)
Security architecture and concepts (design time and runtime)
Enterprise systems
Application layer security
Portals and apps
Devices
Local gateway
Secure local access for service technician
Gateway identity & registration (customization dependent on use case)
Bosch IoT Device Management
Bosch IoT Remote Manager
Backend and cloud runtime
Cloud backup & restore process

3.2. Precommissioning

Device management requires an agent to be deployed on the connected devices. This agent is a software that works autonomously to monitor the devices. It also enables the remote device management software to communicate with the device, for example to send commands and receive responses when required. The agent needs to be configured to automatically connect to the remote device management system with valid credentials for authentication.

3.3. Commissioning

3.3.1. Device registration

An IoT device must be registered in the system before being connected and authenticated for the first time. Devices are usually identified based on serial numbers, preshared keys, or unique device certificates issued by trusted authorities.

3.3.2. Initial provisioning

IoT devices are shipped to customers with factory settings, meaning they don't have any customer-specific software configurations, settings, etc. However, a device management system can match the user to the IoT device and perform an initial provisioning process in order to automatically deploy the required software components, configurations, etc. without any user involvement.

3.3.3. Dynamic configuration

IoT applications can start off very simple and become more mature and complex over time. This may require not only dynamic software updates but also configuration changes to be carried out without involving the user or disrupting the service. Deploying new logic or performing service application updates should be completed without any downtime. Dynamic configuration may apply to only one specific IoT device, a group of IoT devices, or all registered IoT devices.

3.4. Operations

3.4.1. Monitoring

With the complex IoT device landscape, it is necessary to have a central dashboard that displays an overview of the devices and has the ability to configure notification rules based on device status or sensor data. Because of the scale and diversity of the assets, being able to flexibly and dynamically create groups of devices using specific criteria is important for efficient operations and the monitoring of your fleet.

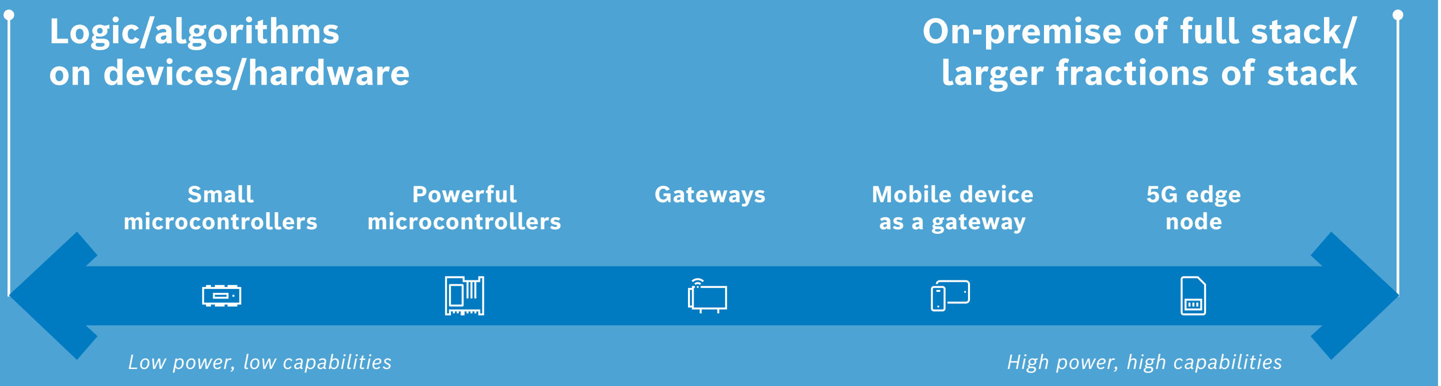
As for the devices themselves, it is also important to have a watchdog to ensure that, in the event of a malfunction, they can at least automatically reboot themselves – or, preferably, troubleshoot the problem autonomously.

3.4.2. Manageable device types

IoT deployment scenarios can vary depending on the domain and application. Modern edge devices differ in terms of capabilities and connectivity methods and an IoT solution must support a variety of target platform types.

Enterprise IoT solutions often have to deal with smaller types of edge devices, which have limited capabilities and cannot be connected directly over the internet, but rather through a gateway. In the following section, we list the most common types of IoT devices:

[Figure 4]


Logic/algorithms on devices/hardware
On-premise of full stack/ larger fractions of stack
Small microcontrollers
Powerful microcontrollers
Gateways
Mobile device as a gateway
5G edge node
Low power, low capabilities
High power, high capabilities

1. Small microcontrollers

Small microcontrollers are cost-efficient and energy-constrained devices, usually battery-powered, and are very suitable for basic edge capabilities e.g. telemetry use cases. They are customer-specific, usually embedded and the software for them is developed as part of the product-design process. This allows you to reduce the customization needed to make a device IoT-ready. Small microcontrollers support device management capabilities such as remote configuration and firmware update.

- Operating system: Real-time operating systems, such as FreeRTOS, TI-RTOS, Zypher
- Reference devices: ESP boards, STMicro STM32 Nucleo, NXP FRDM-K64F, SiliconLabs EFM32GG-DK3750, XDK Cross Domain Development Kit

2. Powerful microcontrollers
Powerful microcontrollers are similar to gateways in terms of hardware but they differ in terms of software, being rather single-purpose devices. They provide advanced edge computing capabilities, such as resource and device abstraction, history, software and firmware updates, software package management, remote configuration, etc.

- Operating system: Embedded Linux
- Reference devices: B/S/H system master

3. Gateways
Gateways or routers are very common in smart homes, intelligent buildings, and industrial environments. These devices can be very powerful as they need to connect with a multitude of edge devices using different communication protocols. Gateways provide advanced edge computing capabilities, such as resource and device abstraction, history, analytics, software and firmware updates, software package management, remote configuration, etc. You can also perform firmware management on the connected devices through a gateway. They can even be added to the setup at a later stage and may serve different purposes that change over time.

- Operating system: Embedded Linux
- Reference devices: Raspberry Pi, BeagleBone, iTraMS Gen-2A, Rexroth ctrlX

4. Mobile device as a gateway
Modern smartphones can be used as gateways and are very convenient for smart home scenarios. They provide connectivity as proxy for WiFi and Bluetooth LE devices, which require regular updates. When used as a gateway, mobile devices allow updating and remote configuration of the device agent.

- Operating system: iOS or Android
- Reference devices: Mainstream smartphone devices

5. 5G edge node
Suitable for industrial purposes and specific environment needs, 5G edge nodes are often used in data centers on-site, and can be deployed on existing devices as a 5G extension. They provide popular capabilities such as resource and device abstractions, history, analytics, software and firmware updates, remote configuration, software package management, etc.

- Operating system: Linux
- Reference devices: x86-powered hardware

A device management system must be able to manage a mix of all these types of IoT devices, which can be connected through diverse network protocols such as HTTP, MQTT, AMQP, LoRaWAN, LwM2M, etc. In certain cases, it may also be necessary to implement proprietary management protocols.

Here is a brief description of some popular connectivity protocols:
MQTT
A lightweight publish/subscribe IoT connectivity protocol, useful for connections with remote locations where a small code footprint is required. MQTT can perform certain device management operations like firmware updates and is available for different programming languages such as Lua, Python, or C/C++.

LwM2M
A device management protocol designed for remote management of constrained devices and related service enablement. It supports device management operations such as firmware updates and remote configuration. It features a modern architectural design based on REST, defines an extensible resource and data model and builds on the CoAP secure data transfer standard.

LPWAN protocols (LoRaWAN, Sigfox)
IoT protocols suitable for constrained devices in wide area networks such as smart cities. Due to their power saving implementation, they fit in well for use-cases where battery capacity is a limited resource.

3.4.3. Mass device management

Mass device management, also known as bulk device management, is often overlooked in smaller IoT deployments that have not yet scaled up. Simple device management measures may suffice at first, but will be limiting as IoT projects with various devices grow in size and diversity. Being able to easily create dynamic hierarchies and arbitrary logical groupings of assets, so that device management measures can be applied on a large scale, will help increase deployment and maintenance efficiency. Such measures can range from firmware and software updates to the execution of complex scripts that take into account the input from the individual devices. In addition, mass device management measures may be fine-tuned through a number of execution scenarios – set up as one-time tasks or recurrent and automated rules, launched instantly and unconditionally or triggered by predefined events, schedules, constraints, and conditions. Such a key functionality will also be of advantage when the development team carries out A/B testing and campaign management.

3.4.4. Software and firmware management and updates

Device management requires the ability to centrally update software and firmware on globally distributed devices. This includes pushing firmware to the device fleet, and – with the advent of complex edge processing – pushing software packages independent of firmware packages. Such software rollouts need to be staged across a group of devices to ensure reliability even when connectivity breaks down. Future-proof IoT solutions need to be able to update over the air, as most assets are deployed in remote environments distributed around the globe. For effective ongoing software and firmware maintenance, it is critically important to be able to create custom logical groupings and automate these tasks.

Bosch IoT Remote Manager

Did you know? Bosch IoT Suite is the core enabler of Daimler's firmware over-the-air updates. Some four million car owners already receive new versions of vehicle software – for example, infotainment system updates – conveniently and securely via the cellular network. This means they no longer have to visit their dealer solely to get a software update. Bosch IoT Suite is the communication hub for vehicles on the receiving end of wireless updates.

3.4.5. Remote configuration

Being able to modify configurations remotely is crucial for the operations team. Once rolled out, devices in the field need to be updated often so that they keep pace with the ecosystem's evolution. This may include anything from changing cloud-side URLs to reconfiguring client authorization, increasing or decreasing reconnect intervals, etc. Mass management features complement all configuration-related jobs, as the ability to trigger mass measures based on complex rules and to run them at scheduled times in a repeatable manner is of paramount importance for operations.

3.4.6. Diagnostics

IoT deployment is an ongoing process that involves constant monitoring and diagnostics with the aim of minimizing downtime and streamlining operations. When devices are in remote locations, access to administrative audit logs, device diagnostic logs, connectivity logs, etc. is one of the most vital features for troubleshooting. If further analysis is required, the device management system should be able to remotely trigger verbose logging and download the log files for analysis, saving valuable time and improving operations efficiency.

3.4.7. Integration

Unless adopting a ready-to-use service, enterprise IoT solutions will usually require access to device management capabilities through a rich set of APIs, which make it possible to integrate external services or customize user interfaces and workflows. In times of open-source development, providing REST and language specific APIs such as Java API is a standard to fulfill remote connection and management use cases.

3.5. Decommissioning

Decommissioning might affect the whole IoT solution or only dedicated components; for example, replacing or decommissioning a single device. Certificates should then be revoked and other confidential or sensitive data should be deleted in a secure manner.

4. Conclusion

Making the Internet of Things a reality is a transformational journey that inspires multiple business innovations.

Given the rising number of IoT innovations, it is critical for enterprises to select the optimum device management platform right at the beginning of this journey. This platform needs to be able to cope with the heterogeneity and diversity of a constantly evolving enterprise IoT landscape and has to be capable of managing the growing number of connected devices throughout their entire life cycle.

Bosch IoT Suite is a complete, flexible, and open-source-based software platform for IoT solutions. It provides scalable and feature-rich services to address device management scenarios throughout the whole device life cycle, including asset and software management. Bosch IoT Suite addresses device management with dedicated solutions for on-premise and for cloud deployments.

Your products for IoT device management

Bosch IoT
Device Management

Manage all your IoT devices easily and flexibly in the cloud throughout their entire life cycle

Bosch IoT
Rollouts

Manage and control software and firmware updates for IoT devices in the cloud

Bosch IoT
Remote Manager

On-premise device management, monitoring and software provisioning

Customer case study ⓘ

Want to start an IoT initiative? You need device management. Customer case study: Smight’s IoT initiative

Directly bookable and equipped with user-friendly UIs, our device management solutions can be used right away, but also allow full integration through modern APIs. In addition, our professional services teams have been enabling customers to manage IoT devices for many years. We have the experience and expertise to assist you in your IoT journey and operationalize your IoT ideas, while you concentrate on what is important for your business. You can focus on IoT application development that adds value, rather than on IoT platform development, hosting, and maintenance. Grow quickly from prototyping to operating as a full-scale IoT-enabled enterprise with Bosch IoT Suite.

ⓘ Try the device management capabilities of Bosch IoT Suite with our free plans

Bosch in the Internet of Things

We believe that connectivity is more than just technology – it's part of our lives. It improves mobility, shapes the cities of the future, and makes homes smarter, industry connected, and health care more efficient. In every sphere, Bosch is working towards a connected world.

As a major device manufacturer, we have experience with millions of connected and managed devices in diverse industries. Thus we know the challenges involved in IoT deployments by heart and the wide range of device management use cases that are addressed.

We have developed a device management solution that enables you to stay on top of the heterogeneity and diversity of constantly evolving devices and assets, thus ensuring that your IoT solution stays up and running as technology evolves.

Free plans: **Test** Bosch IoT Suite for free

Request a live demo

Follow @Bosch_IO on Twitter

Follow @Bosch_IO on LinkedIn

Europe

Bosch.IO GmbH
Ullsteinstraße 128
12109 Berlin
Germany
Tel. +49 30 726112-0

www.bosch.io

Asia

Bosch.IO GmbH
c/o Robert Bosch (SEA) Pte Ltd.
11 Bishan Street 21
Singapore 573943
Tel. +65 6571 2220

www.bosch.io