SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution,Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade,Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19ECT213- IoT SYSTEM ARCHITECTURE
II ECE / IV SEMESTER

IoT Applications in Device Management

IoT device management is defined as the collection of processes, tools, and technologies that help you provision, monitor, and maintain the growing sprawl of connected objects (also called the internet of things endpoints or edge devices) in your home or enterprise network.

As more and more devices come with network capabilities, the demand for IoT device management software is on the rise. According to the Cisco Annual Internet Report (2018–2023), there will be 29.3 billion networked devices by 2023 – that is, 3.6 devices for every person on the planet.

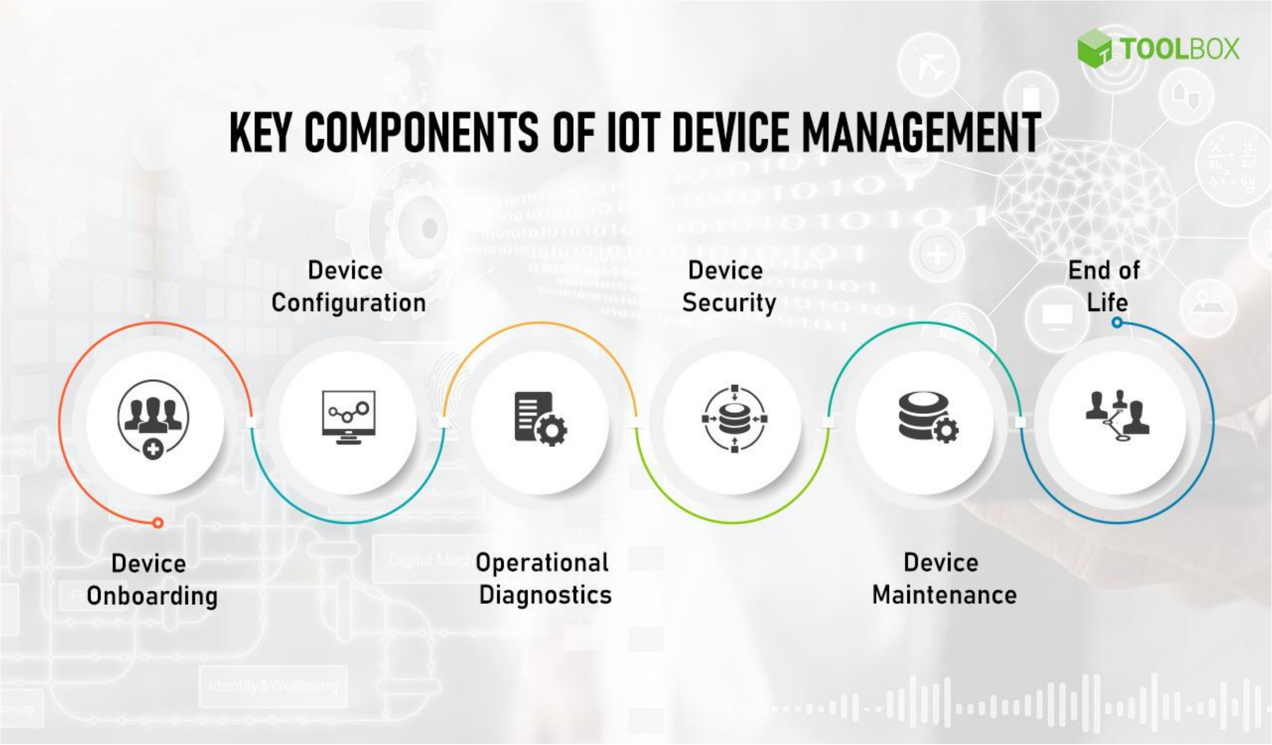
Two factors make IoT device management so important: pull and push.

1. There is a clear pull factor, as intelligent IoT device management paves the way for smarter analytics, more seamless automation, internal efficiencies, and innovative business models. Business models like servitization (where equipment is leased out and services are rendered based on IoT data instead of outright equipment sales) hinge on IoT device management.

2. Further, there is a push factor, as consumer adoption of connected devices is constantly growing. Without IoT device management, employees are likely to keep adding new endpoints to the organizational network, creating a massive shadow IT burden.

For these reasons, a 2020 research report by Valuates Reports indicates that the demand for IoT device management will grow at a 22.6% compound annual growth rate (CAGR) between 2021 and 2026. By the end of this forecast period, IoT device management will be a $6.25 billion market globally.

As mentioned, IoT device management comprises both the processes and the technologies you need to govern your IoT landscape. Some of the key processes necessary across the lifecycle of an IoT device are:



- **Device onboarding**: When an IoT device is switched on for the very first time, it needs to be onboarded into the network. But unlike traditional devices, they do not come with a full-fledged, independent interface to navigate the onboarding process. Checking credentials, defining authentication protocols, assigning a device identity, etc., are some of the steps you could expect in device onboarding.

- **Device configuration:** Every IoT device on your network must be configured as per your business needs. For example, in the case of a fleet of connected trucks, you might want to group specific devices together as per their usual destination or area of operation.

- **Operational diagnostics**: Diagnostics can reveal a host of useful insights into your IoT operations. Most IoT devices would not have sufficient memory or computing resources to analyze diagnostics on the device itself, which is why you need a centralized IoT device management capability.

- **Device security**: This will become an increasingly important part of IoT device management. In 2020, as much as 98% of IoT device traffic in the U.S. was allowed to pass through unencrypted channels, despite comprising 30% of all endpoints. IoT device management brings unmapped endpoints into the organizational oversight and applies necessary security protocols.

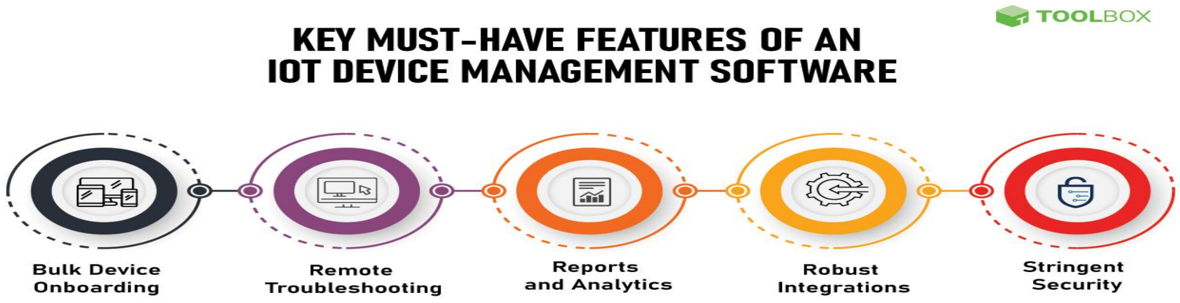
- **Device maintenance:** Apart from updating device firmware to the latest version, you should also watch out for any security vulnerabilities that might creep in unnoticed via fresh releases. IoT device management uses over the air (OTA) updates for device maintenance, and like onboarding or configuration, this is also performed in bulk.

- **End of life**: IoT devices that aren't in use but continue to be part of the enterprise network pose a massive security risk – an external entity could capture data via the device without anyone noticing. Further, an outdated or non-functional device could cause severe operational damage. End-of-life policies and processes specify exactly how an IoT device is to be retired, what are the decommissioning steps needed, and how to recycle the materials for a minimal carbon footprint.

To orchestrate these various processes, you need centralized IoT device management software.

Key Must-Have Features for IoT Device Management Software

To complement your processes and enhance them, the following key features are necessary for IoT device management software:



Key Must-Have Features of an IoT Device Management Software

-
- **Bulk device onboarding**: The software must enable onboarding using a network key and identification credentials. Device onboarding must be performed remotely to establish a secure connection between the endpoint device and the IoT service.
- **Remote troubleshooting**: There should be support for remote troubleshooting to quickly resolve user issues and reduce manual efforts. An integrated governance portal can help resolve issues across multiple endpoints in a consolidated manner.

- **Reports and analytics**: IoT devices typically ship with some edge analytics capabilities. The IoT device management software will be able to display detailed analytics insights in real-time via GUI dashboards. This data can also be converted into reports for business user understanding.

- **Robust integrations**: Compatibility with your hardware ecosystem and application codebase (i.e., the language in which they are written) is an essential feature for this software. It must connect with downstream data servers and enterprise apps for integrated workflows.

- **Stringent security**: The software should equip you with detailed device logs to detect instances of anomalous use and unauthorized access. Real-time notifications sent via the software's dashboard can help diagnose issues and conduct root-cause analysis quickly.

While these are the must-have features to look for, you should also prioritize value-added services that augment the potential of your IoT devices. For example, the solution might come with application development capabilities that let you build your very own IoT apps (complete with cloud-hosting) and further grow your business. Or, you could integrate artificial intelligence (AI) and machine learning (ML) to make IoT device management more contextual – i.e., analyzing diagnostics data against other infrastructure KPIs to understand the best operational configuration.

Recognizing these possibilities, the world's leading IoT device management software providers offer unique differentiators that make these solutions suited to specific business requirements. Let us assess some of these solutions.