The Three Different Software Applications Every OEM Must Develop (And Why You Shouldn’t)

Table of Contents

Introduction 1

Why Connected Devices and Machines Need Three Different Device Management Software Applications 2

The Challenge: Building Three Different Device Management Applications is a Real Pain 3

Benefits of an Industrial-grade Ready-to-use and Customizable Multi-tenant Device Management Software 5

MACH10 Global Device Manager: A Multi-dimensional Industrial-grade Device Management Software for OEMS 5

LANTRONIX

Introduction

The Internet of Things is enabling digital transformation across all industry verticals and is driving the need for more connected devices and machines than ever. As stated in our previous whitepaper, "Busting the Myths of OEM IoT Application Development," one of the key must-haves for today's connected devices and machines is a robust suite of software applications that help realize the productivity and workflow advantages of a true "IoT solution".

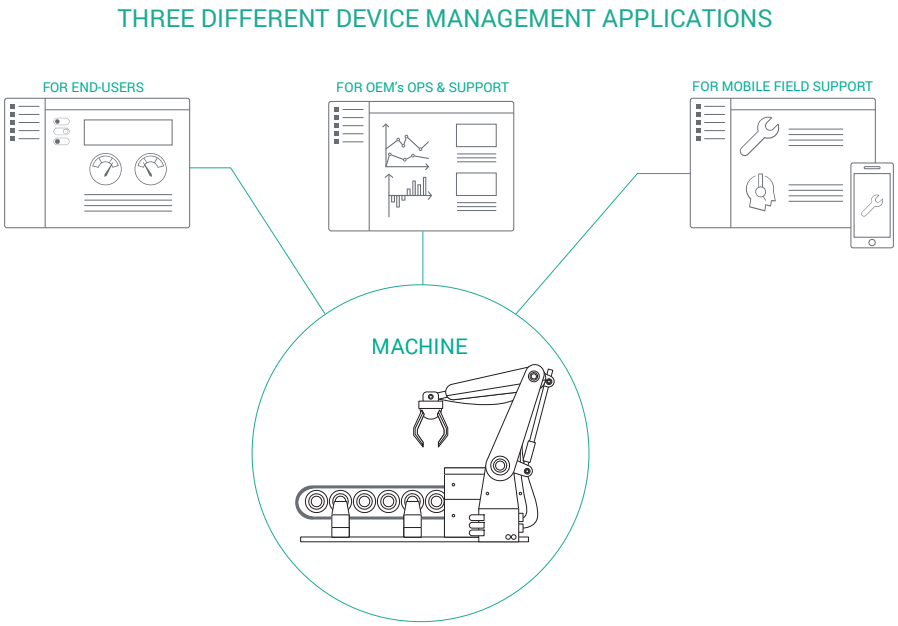
Today, building a smarter connected device or machine requires more than just developing the firmware. An OEM's development teams are under pressure to develop and deliver more software applications quickly to satisfy customer's needs and stay competitive. While the number and types of software applications may vary between different OEMs and types of devices, every OEM needs to develop these three different software applications for their connected device and machines:

- Device management software for end-users
- Device management software for OEM's operations and support teams
- Device management software for field support teams

These software applications allow multiple stakeholders and a variety of users - from the OEM to the system integrator to the field support technician to the end-user to securely provision, operate and maintain the connected devices and machines, ultimately leading to improved outcomes such as enhanced productivity, improved quality and reduced costs.

Why Connected Devices and Machines Need Three Different Device Management Software Applications

Different stakeholders interacting with a connected device or machine have different needs. Further, different stakeholders must be within different trust zones for security and privacy reasons.



Device management software for end-users

- Provision and configure the connected devices or machines
- Operate the connected devices or machines
- Integrate data from the connected devices or machines with other line of business applications

Device management software for OEM's operations and support teams

- Centralized firmware and configuration updates
- Remote diagnostics and support
- Device data collection and predictive maintenance

Device management mobile application for field support teams

- Directly connect to devices or machines for quick diagnosis
- Connect to centralized device management software for device or machine history and documentation
- Re-configure and provision devices or machines

The Challenge: Building Three Different Device Management Applications is a Real Pain

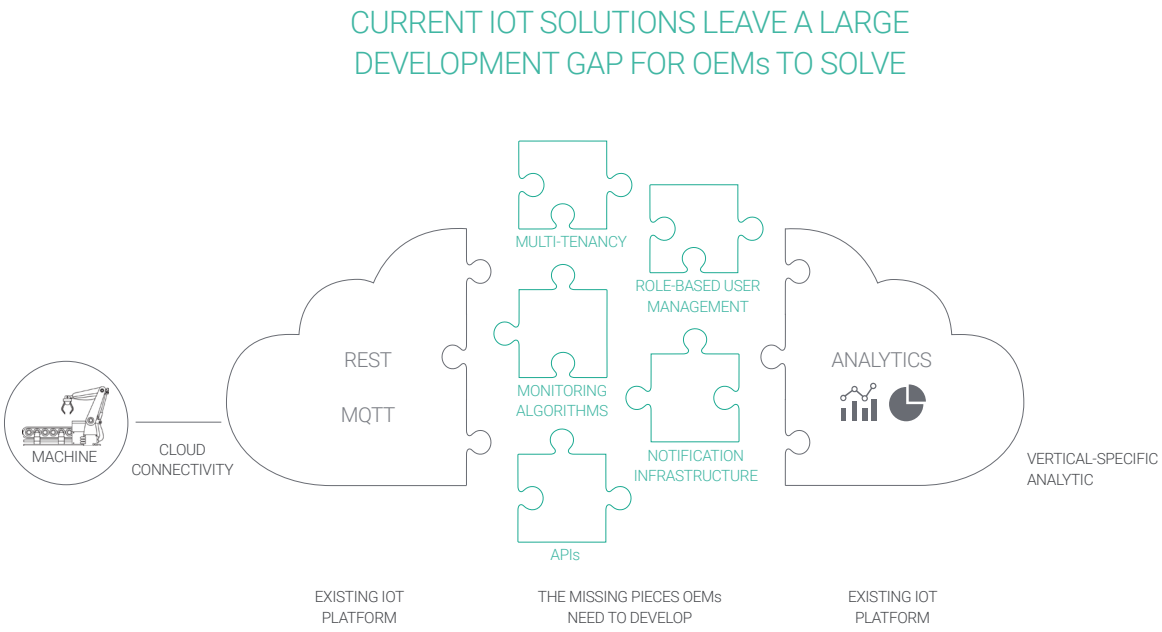
Developing software that runs on a single device is very different from developing device management software that provisions, operates and maintains thousands of devices. In addition to reliably orchestrating thousands of devices simultaneously, every type of industrial-grade device management software must deliver the following functions at the very least:

- User management
- Role-based access controls
- Automated monitoring and notification infrastructure
- Data management
- API gateways
- Billing
- Security, privacy and trust management

These are capabilities that must be built into every type of device management software, whether it is for the end-user, the OEM's operations and support teams or field support technicians.

Most existing IoT platforms either provide cloud connectivity at scale or vertical-specific data analytics leaving everything in between that is required for building industrial-grade device management applications to the OEM's development teams to develop, deploy and maintain.

Platforms such as Amazon AWS and Microsoft Azure provide useful IT building blocks for connecting devices and machines to the IoT cloud. These include virtual machines, databases, message busses, to name a few, as well as REST API and MQTT connectivity at scale. While device connectivity is an important first step, platforms that are predominantly IT-oriented still leave an OEM's development teams with much of the legwork of developing the IoT software necessary to develop the fundamental device management functions, such as user management with role-based access controls, device directories and views, real time monitoring algorithms and notification logic, API functionality, UI/UX design and web applications.



On the other end of the spectrum are other platforms that require OEMs to either toss out their prior software investment and/or limit functionality to their own connectivity hardware. This element ends up limiting an OEM's ability to deliver scalable device management software to their support partners or customers, and in many cases, makes this task virtually impossible without significant additional investment.

Developing and maintaining the different industrial-grade device management applications requires large CAPEX and OPEX budgets, as well as a team of dedicated resources with specialized talent and understanding of both the IT and IoT software elements needed. Many large and small OEMs struggle with balancing these demands against the continuing investment required for evolving their own core competencies.

A single ready-to-use industrial-grade device management application that supports multi-tenancy, multiple user types and role-based access control to capabilities, flexible deployment options and customizable by the OEMs to meet their unique needs, look and feel would be ideal. Such an application would eliminate the need for developing three different device management applications from scratch for different stakeholders. Further, it would dramatically reduce the cost, complexity and uncertainty while accelerating time-to-market.

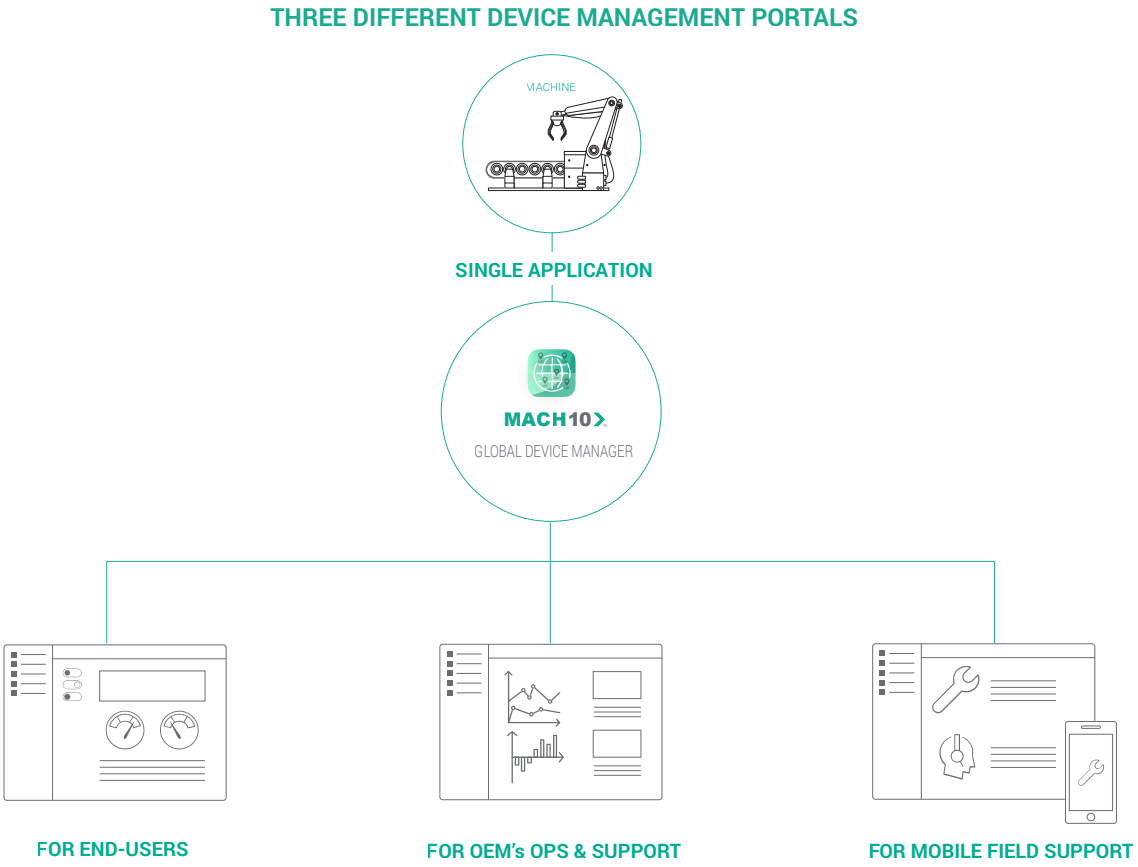
Benefits of an Industrial-grade Ready-to-use and Customizable Multi-tenant Device Management Software

A single ready-to-use and customizable multi-tenant device management software with support for multi-user role-based access control and flexible deployment options allows the OEMs to get to market faster with their connected devices and machines. There is no need to develop three different device management applications, one for each group of stakeholders.

- *Multi-user role-based access controls* enable different capabilities for different users types. This means that a single device management application can be deployed for different stakeholders interacting with a connected device or machine, instead of developing three different device management applications
- *Multi-tenancy* enables OEMs to deploy a single device management application for their entire global customer-base. Multi-tenancy helps keep devices and data isolated between OEM's customers, with all data secure and private
- *Flexible deployment options* allow the device management application to be hosted by the software vendor in the cloud or OEM's private cloud or on-premise at OEM's customer site.
- *Industrial-grade* device management applications come with long term availability and support, usually from well-established reputed companies that have been providing solutions that meet the demand of the industrial segment
- *Customization* capabilities enable the OEM's development team to configure the single device management software for multiple stakeholders, including access levels, capabilities, look and feel, including OEM and end-user branding

MACH10™ Global Device Manager: A Multi-dimensional Industrial-grade Device Management Software for OEMs

Lantronix MACH10™ Global Device Manager is a single industrial-grade ready-to-use device management application suite that is available as a hosted solution or for deployment in OEM's private cloud or on-premise alongside with their existing management software applications to provision, operate and maintain their connected devices and machines.



Instead of developing three different device management applications for different stakeholders, MACH10 allows OEMs to configure different self-service web portals for different stakeholders. A web portal enables OEMs to enable a set of capabilities for a group of users or for a group of devices. Because web portals can be enabled for self-service use, OEM's end-users can create their own accounts, import devices and interact with them based on the functionality that has been authorized by the OEM. OEMs can now create a self-service portal for their global customer-base to self-register their users and devices they purchased or will purchase in the future. Additional web portals can be created for system integrators, partners, and field service teams, all with different levels of access to devices, management and maintenance capabilities depending on their roles and responsibilities.

For example, the three web portals that an OEM can create are:

Device management web portal for end-users, allowing the end-users to:

- Provision and configure the connected devices or machines at their locations
- Operate those connected devices or machines
- Integrate data from those connected devices or machines with other line of business applications

Device management web portal for OEM's operations and support teams, allowing them to:

- Centralize firmware and configuration updates for all the devices deployed by all of their end users
- Remote diagnostics and support
- Device data collection and predictive maintenance

Device management portal for field support teams

- Directly connect to devices or machines for quick diagnosis
- Connect to centralized device management software for device or machine history and documentation using the native mobile application that connects to the device management portal with secure APIs
- Re-configure and provision devices or machines

For OEMs who would like to augment their existing management software applications with MACH10 Global Device Manager capabilities, MACH10 Global Device Manager provides a powerful suite of secure and authenticated APIs. MACH10 Global Device Manager can run entirely in the background while augmenting OEM's existing management software without the need for reinventing the wheel. These robust APIs also enable OEMs to jumpstart development of their custom device management applications.

As an IoT OEM building for OEMs, Lantronix designed MACH10 Global Device Manager as a contemporary IoT application suite that allows OEMs to deliver a more complete IoT solution that can benefit all stakeholders. For more than two decades, Lantronix has built a strong reputation for providing OEMs with industrial-grade solutions with production ready software that simplify connectivity and "just work". Many Fortune 1000 customers trust Lantronix products for their reliability and security, and rely on them for even the most mission critical applications. Today, Lantronix is focused on continuing to help companies *Connect Smart and Do More* by leveraging our 28 years of extensive knowledge and experience in bringing IT management capabilities to the OT to create a complete portfolio of solutions that allow industrial OEMs to go to market faster and simplify execution of their IoT initiatives.

LANTRONIX®

CONNECT SMART. DO MORE.

www.lantronix.com

Corporate Headquarters
Lantronix, Inc.
7535 Irvine Center Drive
Suite 100
Irvine, CA 92618
Tel. 949.453.3990