IoT Connected Devices

As wireless connectivity and low-cost, low-power sensor technologies continue to advance, more and more devices are being enhanced with internet capabilities. This has created an entire *Internet of Things* (IoT), able to send and receive information with other devices directly over the internet.

IoT goes well beyond mobile devices and tablets; today's connected devices include everything from smart smoke detectors to wearable health monitors. And businesses are no exception; most modern organizations incorporate entire fleets of IoT devices for tasks such as data collection, routing, and edge computing. But with the expanded capabilities the IoT brings to businesses, there is also the potential for them to create problems if not managed correctly.

IoT management provides the solution, allowing organizations to better monitor and control their essential IoT devices, and to employ insights from IoT data in decision making and strategy development.

What are the fundamentals of IoT device management?

The basic requirements of IoT device management can be broken down into the following five categories:

Onboarding

For a device to become part of the IoT, it first needs to be properly connected to the internet. In terms of IoT device management, the onboarding stage consists of *authentication* and *provisioning*. Authentication includes verifying the credentials of every proposed device, rejecting those that do not meet authentication standards. During authentication, the device establishes a secure connection between itself and the IoT system or platform, and if its credentials are valid, it receives additional configuration data. Provisioning is the overall process of enrolling the device into the system. Effective provisioning is not only a necessary step for new businesses trying to get up and running quickly; it's also essential to accelerating time to market on specific projects and ensuring that new devices don't open the organization up to attack.

Configuration

Although most devices are shipped with some level of standard preconfiguration, it is unlikely that these 'factory settings' are the optimal configurations for the organization or the specific use case (such as the device's deployment location or its role). IoT device management must be capable of further configuring connected devices to better function within the organization's IoT ecosystem.

Maintenance

Even properly authenticated and configured IoT devices may not remain positioned to function optimally over long periods of time. Firmware updates might introduce bugs, new security vulnerabilities may be discovered, or the scope of certain projects may simply change. IoT maintenance exists to ensure that these devices in the field may be updated when needed, so that they remain current and secure.

Diagnostics

Going hand in hand with maintenance, IoT diagnostics allow organizations to closely monitor their connected devices to reduce the risk of downtime, security failures, firmware bugs, etc. At the same time, proper diagnostics gives companies the information they need to employ *predictive maintenance*, incorporating advanced analytics and revealing key insights and root causes, before small issues can grow into significant problems.

End-of-life management

Taken together, onboarding, configuration, maintenance, and diagnostics are capable of supporting and optimizing IoT devices throughout their entire use life. But what happens when that use life is ended? When projects reach completion or individual devices become obsolete, IoT device management is responsible for decommissioning devices in a way that is both secure and cost effective. Often, replacement devices must also be prepared to step in and take over for the decommissioned ones. The goal of end-of-life management is to minimize the risks of data leaks, system downtime, and security issues arising from a temporarily compromised system.

What are key features of IoT device management?

Top IoT device management platforms often include the following features:

- Bulk registering and deploying connected devices

- Organizing devices into relevant groups

- Indexing and searching device fleets

- Device logging

- Remotely managing and updating devices

- Custom scripting

- Security tunneling for diagnosing and resolving issues

- Customizable dashboards for centralized device control

What are the benefits of using IoT device management?

By empowering organizations to better monitor and control their connected IoT devices, IoT device management offers a number of significant benefits. These include the following:

Faster registration of IoT devices

IoT device management provides tools and solutions to shorten the development, configuration, and deployment times of connected devices, essentially making it possible for organizations to get entire networks operational immediately. IoT management can also futureproof architectures, allowing for large-scale future deployments at significantly reduced time and effort.
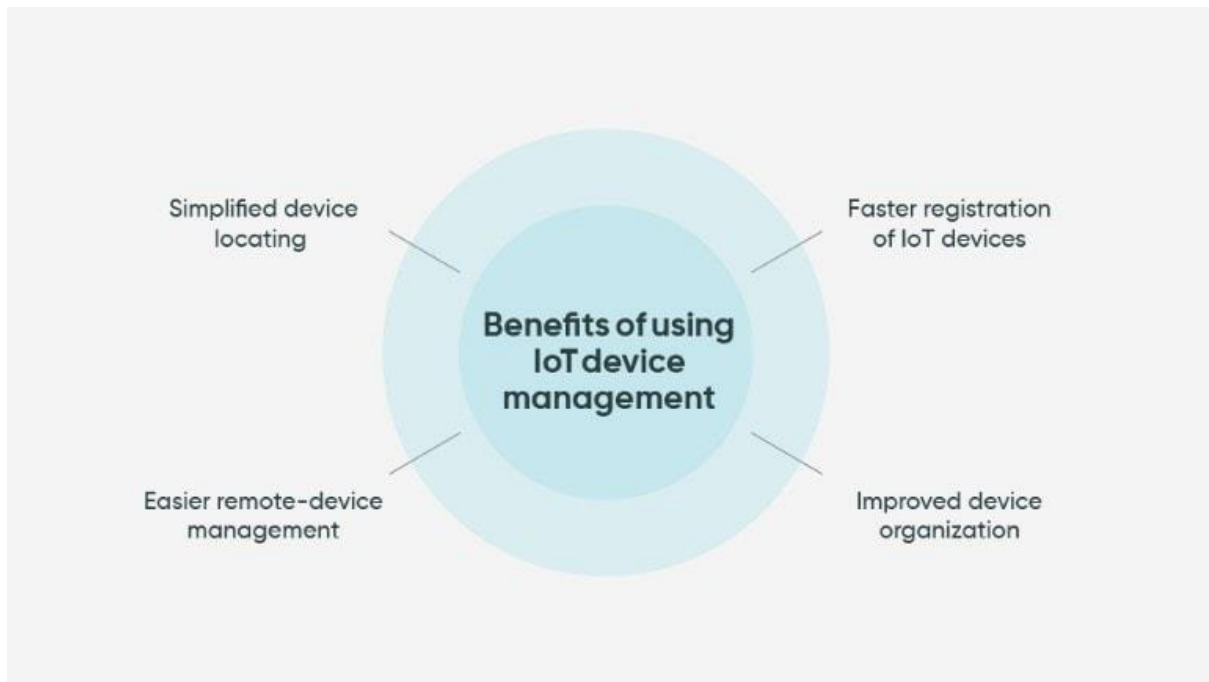
Improved device organization

Effective device management provides the capabilities to organize devices into groups and hierarchies, and to manage relevant access policies for each. This simplifies device tracking and operations and helps more closely align devices with established business and security practices.

Easier remote-device management

Unpatched or un-updated devices in the field can be difficult to access. IoT device management makes it possible to update software remotely, as well as execute security patches, reboots, and factory resets across an entire IoT fleet. And, in the event that individual devices may be experiencing issues, IoT device management allows organizations to access, troubleshoot, and resolve many of these issues completely remotely.

Simplified device locating

When it's necessary to locate a single device from among potentially thousands of IoT objects, IoT device management is capable of using a combination of device attributes to find specific devices in real time. This makes it easier for businesses to troubleshoot and possibly retrieve problematic devices as quickly as possible.

When should businesses use IoT device management?
IoT device management is not limited only to those organizations with extremely large IoT ecosystems; it may be effectively used across a variety of industries and applications. That said, the most-common applications include the following:

Industrial

With IoT device management, businesses can connect entire fleets of industrial devices quickly, accurately, and with a minimum amount of effort. Detailed device monitoring makes it possible to track performance metrics and detect potential issues across entire industrial sectors, making configuration adjustments where needed.

Commercial

With IoT device management, organizations can easily group entire commercial device fleets hierarchically, based on a range of categories. These categories include security requirements, function, location, and more. IoT device management also makes it possible to put individual devices under the microscope or take a more-encompassing approach and take actions across an entire fleet.

Consumer

Traditionally, consumer IoT devices are more difficult to manage. IoT device management facilitates effective governance of devices already deployed in the field, allowing organizations to send updates and patches, and to improve device functionality without negatively affecting the user experience.

What does IoT Device Management Enable?
Although the specific capabilities of IoT device management may vary from platform to platform, most IoT device management options generally provide organizations with the following capabilities:

Sending and receiving data

IoT device management acts as a central hub from which to communicate with deployed devices in real time. Operators can send and receive important information, either over the web using the HTTP protocol, or directly between devices with the MQTT protocol.

Executing workflows

IoT management allows organizations to define essential workflows using the data collected by connected devices. Data-defined workflows help promote more effective and efficient actions.

Facilitating maintenance

Properly managed, IoT devices are capable of providing their operators with a steady stream of sensor data. This helps inform the organization of potential issues as they arise. Additionally, many IoT solutions allow organizations to perform regular maintenance and emergency software repairs remotely, often without any significant device downtime.

Taking action

IoT device management brings together related devices, allowing them to take action based on the data they exchange with one another. For example, if a climate control sensor detects a change in room temperature, it can send that data along to the relevant HVAC unit, which will then automatically take action to maintain the desired temperature.

Performing analysis

Once the devices are connected, IoT management allows organizations to monitor devices in association with operations and business, visualize and analyze incoming data, measure telemetry, and then use data insights to take action. Companies can also optimize their assets based on IoT monitoring, look at historical trends over time, and perform root-cause analyses to detect issues with critical equipment and data.

ServiceNow for improved IoT device management
IoT device management is vital for organizations fielding fleets of connected devices, but it's only the beginning. With ServiceNow, you can combine IoT data with your workflows to enable proactive maintenance, greater uptime, and increased customer satisfaction.

Built on the award-winning Now platform, ServiceNow Connected Operations gives organizations the ability to easily and quickly turn IoT data into actionable insights. Enjoy increased visibility and monitoring across multiple sites and customers, apply rules and business context to identify problems in real time, and connect relevant teams and departments through a centralized location.

Across the world, the Internet of Things is expanding to encompass more and more connected devices. ServiceNow gives businesses the power to expand along with it, with effective, data focused IoT device management. Learn more about ServiceNow Connected Operations and get more out of your connected devices