IOT DEVICE MANAGEMENT: SECURE AND SCALABLE DEPLOYMENTS

WITH DIGI REMOTE MANAGER®

INTRODUCTION TO IOT DEVICE MANAGEMENT: SECURE AND SCALABLE DEPLOYMENTS WITH DIGI REMOTE MANAGER®

The Internet of Things (IoT) has paved the way for millions of connected wireless devices to route information and get things done. The enabling technologies of the IoT allow connected devices to gather and send data, handle remote or risky tasks without human intervention, monitor assets to avoid unnecessary service calls, and gather critical information from widely dispersed and demanding environments.

To effectively manage a complex IoT deployment requires an IoT device management application that not only lets you visualize the activity of complex networks in a simplified form, but also provides these important capabilities:

- **Management:** Manage large numbers of devices efficiently
- **Monitoring:** Monitor IoT deployments and ensure all devices are operating as expected
- **Security:** Continually scan the deployment for security issues and repair them

These capabilities must be seamless across devices and third party applications from the cloud to the edge of the network. In this white paper we will talk about IoT management paradigms, and how a sophisticated remote management application, paired with a strong security framework, can help manage your connected world more efficiently and securely. We will also introduce the capabilities of Digi Remote Manager® (DRM), the Digi TrustFence® security framework, and the Digi Foundations™ hardware, management and support package.

Challenges in the Management of Connected Devices

The challenges involved in managing IoT devices are many and varied:

- Devices may be difficult to reach, such as those located at the top of a pole, on a remote highway, or out at sea. Once these devices are installed, it is inconvenient and expensive to go back and check on them or service them.
- Devices may be in motion—for example, if they are installed on a delivery vehicle or city bus. You need to be able to communicate with these devices while they are in transit, wherever the vehicle may be located.
- Your device network may be geographically diverse and deployed in large numbers. You need to be able to communicate with and manage devices on a large scale.

When identifying strategies for managing and servicing devices in your IoT deployment, it may help to think about them as being on another planet. Regardless of their locations, you will need to be able to monitor those devices, communicate with them, send commands to them, and update firmware and security patches across your entire network.

In the following sections, we will discuss how to address these challenges across geographically dispersed IoT deployments. We will cover these four topics:

- Managing device networks at scale
- Managing security in your IoT deployment
- Connectivity to the edge
- Stack integration

Managing Device Networks at Scale

With the proliferation of devices across the IoT landscape, managing at scale is increasingly of interest to those who must maintain device networks. If you have deployed a small number of devices, you may find firmware updates and device monitoring to be quite manageable, as you can log into each device individually and make updates as needed.

But if you have hundreds or even thousands of devices all over the world, this changes the management requirements significantly. If you need to update firmware across your network, or you want to roll out a security update to all devices, the challenge is much greater. You would need a large staff to monitor and manage all of those devices manually. Clearly, that doesn't scale. The alternative is to use a sophisticated device management tool that automates a lot of that work for you.

Digi Remote Manager is one such IoT application. This cloud-based service makes it possible to monitor your entire IoT device network from a management dashboard. The dashboard provides a graphical view of your entire deployment, and drills down into various devices or device groups. It also enables you to create rules that govern your monitoring processes.

For example, you can:

- Set alerts that will automatically notify you under certain conditions, such as if any device fails to come online as expected
- Generate reports on the health of the device deployment, either on an individual basis, or for all of your devices in aggregate
- Set up processes to automate the report generation at desired intervals for ongoing evaluation

Additionally, DRM enables you to push software updates to your entire network with just a few clicks. For example, to perform a site-wide firmware update, you can use DRM to create a profile that specifies the new version of firmware or a new configuration. That profile will manage the rollout of those firmware updates to all devices.

In the same way, if you want to ensure that devices on the network comply with certain configuration settings, DRM enables you to push those requirements out to all devices, and then ensures that the devices remain in compliance through automated monitoring.

You can use the same method to roll out other files, such as a Python program, to all devices. DRM will let you know if the updates were successful for all devices, or if any failed for any reason.

Likewise, you can use this methodology to monitor and update your device security configurations.

Managing Security in Your IoT Deployment

IoT security is no longer the elephant in the room. Organizations are actively addressing security issues with their device manufacturers, service providers and IT personnel. Many security issues have been exposed in recent years, leading to updated thinking and multiple advancements in technology and best practices.

IoT security requires more than just making sure a device isn't compromised. It requires a proactive, multi-layered approach, including a plan for what will happen when breaches do occur. For more information on a multi-layered approach to security, see our blog post, *Who Is Responsible for IoT Device Security?*

Digi implements security via a framework called Digi TrustFence®, which is a set of tenets that we apply to our standard practices and the development of our devices. The Digi TrustFence framework incorporates these strategies:

- **Secure boot:** Device firmware and software validation; authenticates that the software came from the manufacturer.
- **Authentication:** Secure identification and authentication methods for managing user and device identities.
- **Secure connections:** Secure encryption protocols to ensure the integrity of data being transmitted over the network.
- **Encrypted storage:** Sensitive file encryption to ensure secure storage of data.
- **Secure updates:** Identification and validation of firmware and software from authorized sources prior to installation into the device.
- **Configuration management:** Ability to define secure baseline configurations and apply them automatically.
- **Protected hardware ports:** Protected, access-controlled internal and external ports prevent unwanted "back doors."
- **Device identity:** Certificate management and secure key storage to protect the identity of the device and the data it collects.
- **Defense in Depth:** Digi uses multiple design methods of securing a device. We anticipate that a vulnerability may happen, and we add alternative controls to significantly reduce the impact of any vulnerability.
- **Ongoing monitoring and support:** Digi has a team devoted to monitoring security issues, performing internal and external security audits, and rolling out security patches to customers.

> IoT security is no longer the elephant in the room.

DRM plays an integral role in each of these framework components, with the exception of secure boot. It supports each of these tenets through monitoring, reporting and automated recovery. For example, some of the capabilities we have touched on enable you to proactively monitor and manage the security of your device deployment, as follows:

- Generate reports on any given device or on your entire device deployment in aggregate, either on demand or on a scheduled basis.
- Create profiles, or policies, that specify the configuration of your devices, as well as files that reside on them. This includes encryption and authentication settings. Once you have created one of these policies, you can implement it using one of these methods:
    - Push the configuration policy out to all devices of the same type in your deployment, simultaneously
    - Configure DRM to monitor all devices across your deployment for any lapses in compliance with the established configuration
    - Receive alerts for any lapses in configuration compliance, and either investigate them or automatically repair the devices and bring them back into compliance
    - Push out new security patches across your device deployment whenever you have security updates

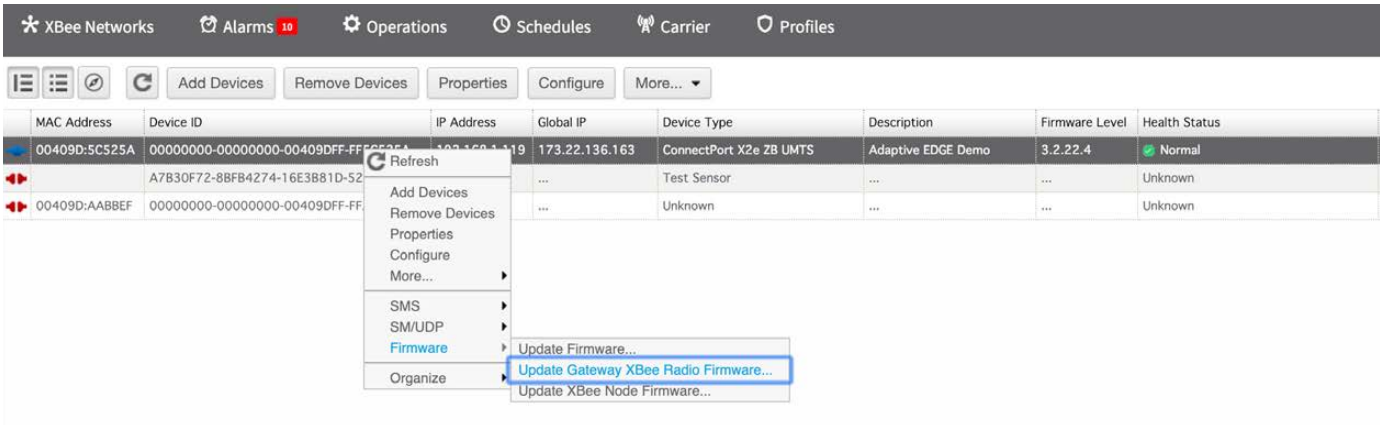
There are a number of ways to establish security across a network, including homegrown security monitoring systems. The methods described are designed to reduce the cost of resources required to monitor and maintain a secure IoT deployment while ensuring a higher level of security that works round-the-clock, 365 days a year. DRM has the added benefit of being able to monitor all of the critical aspects of devices without having to implement something that is custom. So, it is literally, "configure and go."

Managing Connectivity to the Edge

Today, the supporting technologies of the IoT have expanded the playing field for how, where and when we connect, transmit data and perform operations. Depending upon your application needs, you may find it useful to gain access to the edge devices that are beyond the directly connected devices in your IoT deployment. Developing an edge computing strategy can help to optimize your cloud computing environment and improve network load by moving some of the data processing to edge devices, for instance.

As an example setup, you could have a gateway with IP connection capabilities that can connect back to the DRM platform. The gateway can provide a bridge to something like a Zigbee network so you can see the Zigbee nodes associated with the gateway. Using DRM, you can view the configuration settings of the Zigbee devices or make changes to them.

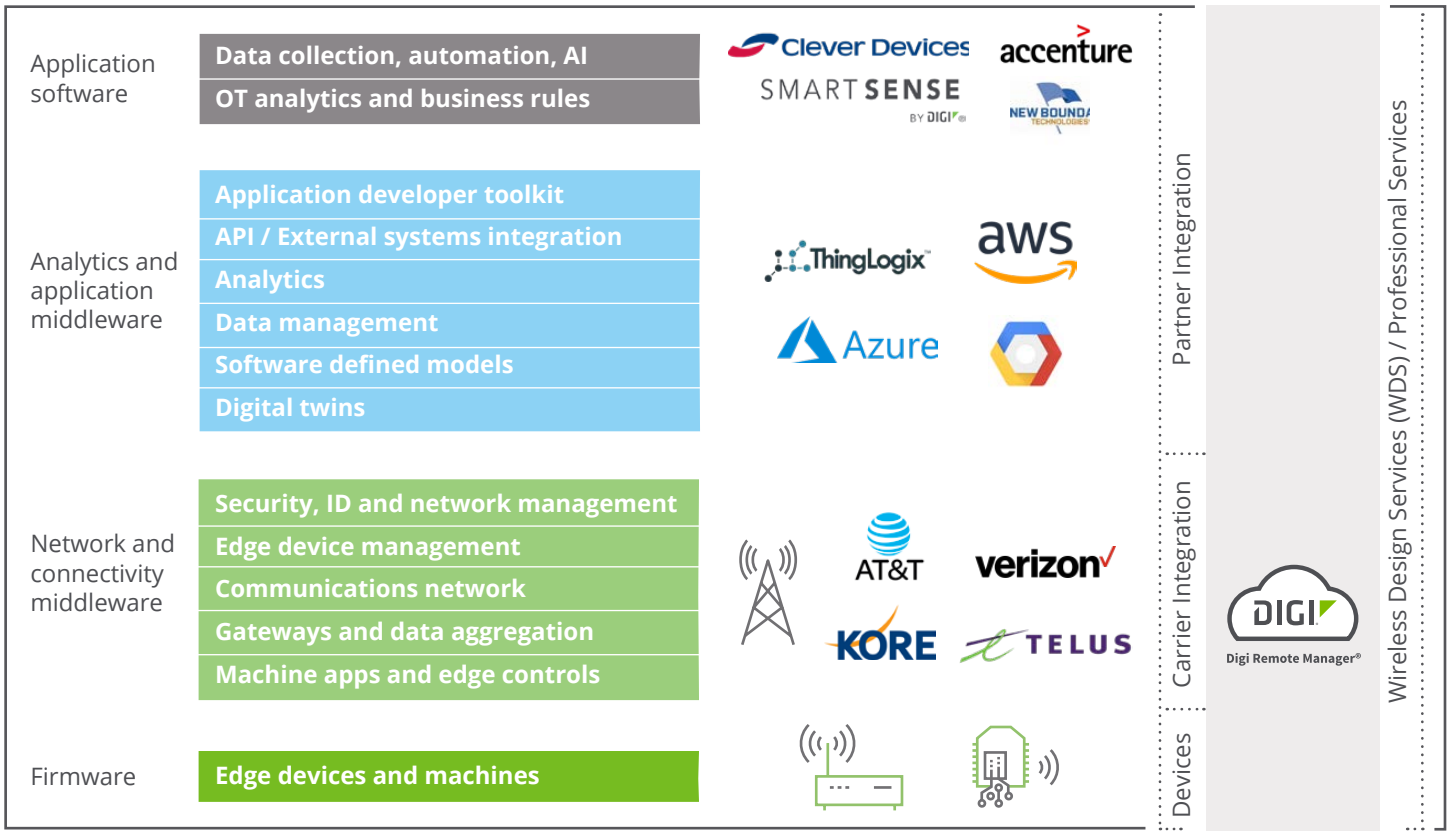
To expand connectivity to your edge devices, use DRM in combination with gateways to monitor and manage devices beyond the gateway. Once this connectivity is in place, include those devices in the monitoring, maintenance, automation and security you have established for your IoT device deployment. For example, upgrade the firmware of the XBee radio in the gateway, as well as the firmware in the remote nodes on the entire Zigbee network simultaneously.



Use DRM to update firmware on edge devices

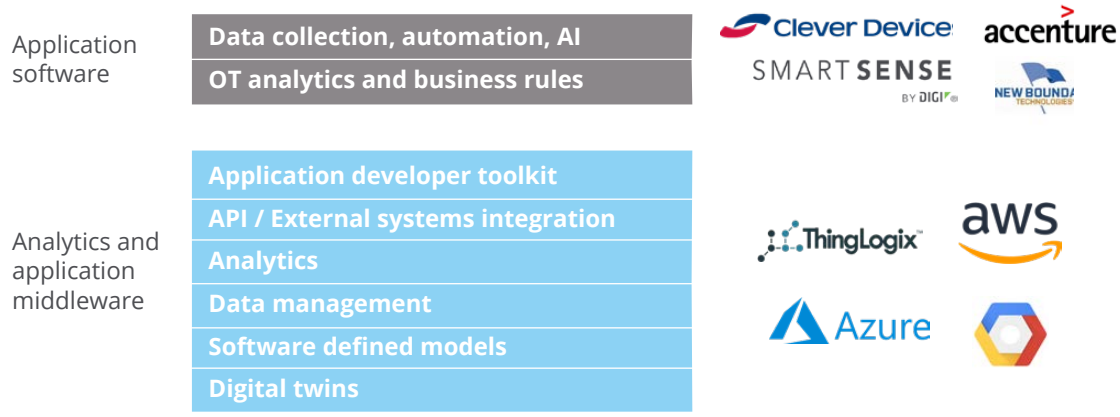
Managing and Integrating the Entire IoT Stack

To pull together all the different pieces of your IoT device deployment, as well as edge devices and even third-party services into one integrated system, it is helpful to view this collection of hardware, software and cloud-based programs as the "IoT stack." The following graphic illustrates the full IoT stack, including applications, tools, middleware and firmware. DRM manages most aspects of the IoT stack, including devices, cellular access with any carrier, and any third-party application middleware.



Building blocks and full stack solutions

We have been primarily discussing the bottom portion of the stack, including the devices in the communication network, gateways and security services. Next we will be talking about the top portion of the IoT stack, where you might integrate with third-party applications or other cloud providers.



The management of all of the stack layers, components and services can get extremely complex when there are multiple devices and you want to connect them to different services like Microsoft, Amazon or Google. The complexity can increase dramatically with a large or diverse device deployment, employing a combination of services. It can be especially daunting if at some point you want to switch to a different provider.

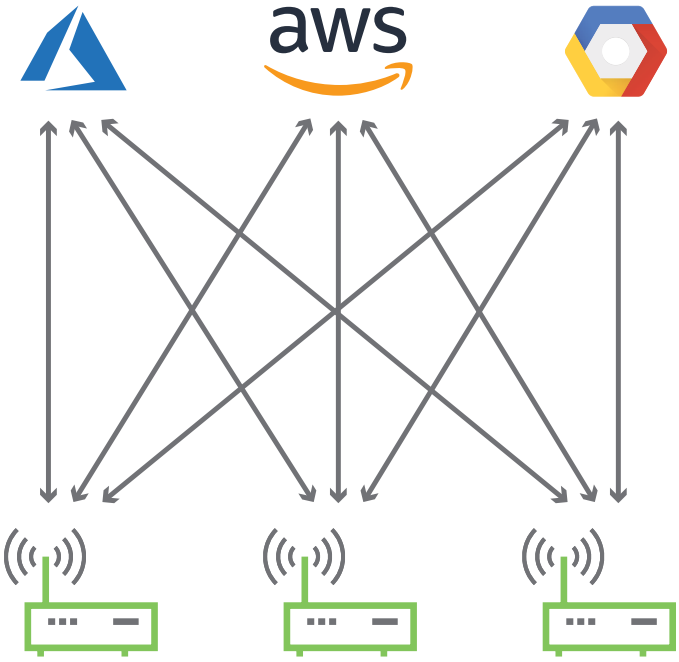
The complexity can increase dramatically with a large or diverse device deployment.

Simplifying IoT Complexity

A central device management platform like Digi Remote Manager makes it much easier to deploy those changes out to all of your devices. DRM actually enables you to integrate with those providers and thus facilitates management of your third-party services. You can choose to have your entire data path going through DRM, or you can choose to send your data directly from the devices to the third-party IoT cloud provider. DRM allows you the freedom to choose the method that works best for youruse case.

DRM can act as facilitator between edge devices such as cellular radios, gateways and routers and third party services such as Microsoft Azure, AWS and the Google Cloud Platform. There are many possible scenarios, depending upon the needs of your application and your specific configuration. But in a nutshell, DRM has the capability of integrating with many different third-party services. It can then simplify your ability to get your data where you want it to go.

For example, DRM can push firmware updates and other code, including security patches, Python code and updates from third-party applications, out to your entire installation of deployed devices. It also provides visibility into the health of those devices, and can route that data wherever needed. And in the event that an entire deployment must be rerouted from one third-party cloud application to another, DRM has the ability to deliver the new code to all devices in the network for a seamless switchover.



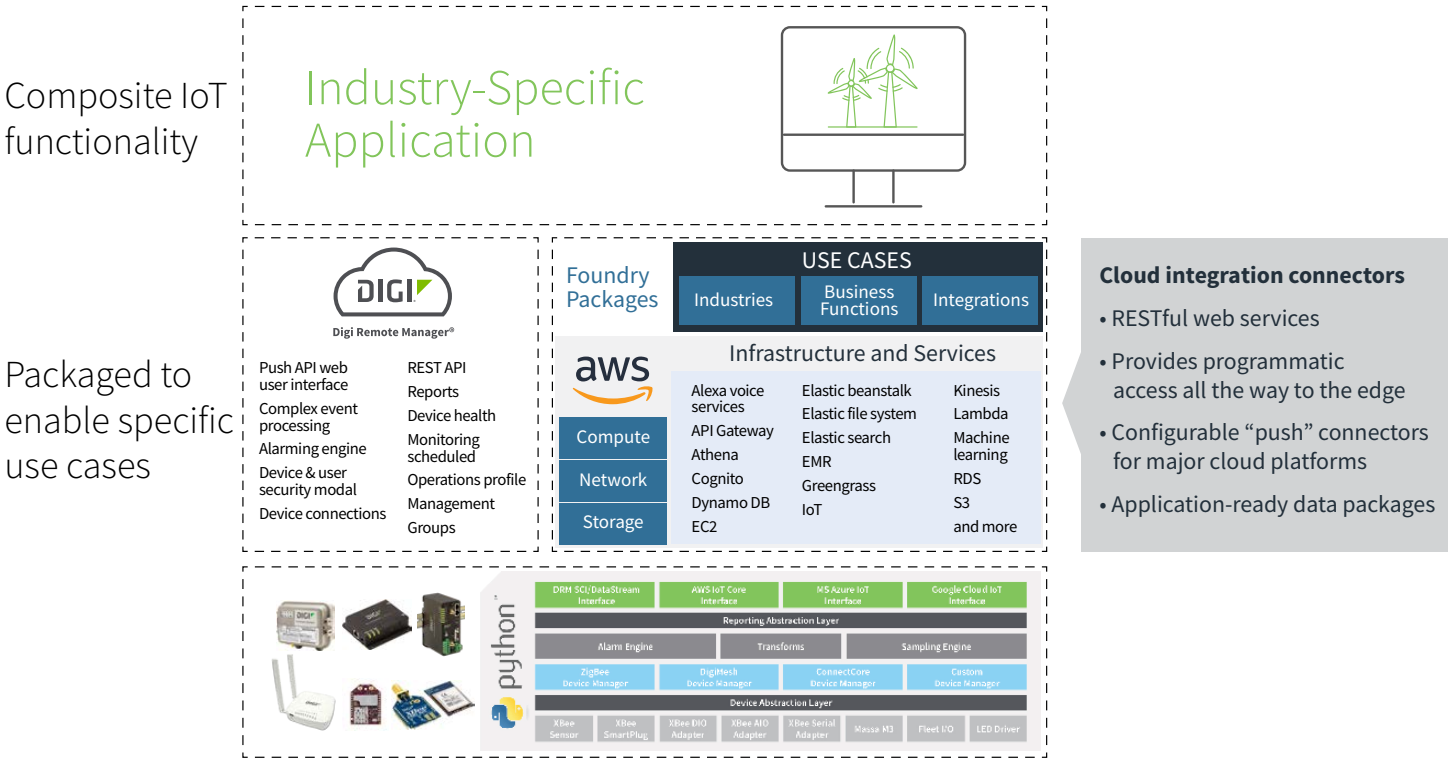
IoT complexity

DRM simplifies IoT complexity

Managing Integration Complexity

To integrate DRM with third-party IoT cloud providers, we use the RESTful web services interface of DRM. While it has a dedicated connection to the devices at the bottom layer, it provides the ability for third-party applications to access all of the functionality of those devices, as well as the automated functionality of DRM, via web services.

For example, you could push Python code out to your devices that would allow you to connect to the third-party providers using one of several protocols, such as MQTT or HTTP. This makes it very easy if you decide at some point that you want to switch third-party IoT cloud providers. Since DRM integrates with those providers, but operates independently, it can help you manage the connectivity to your cloud platform of choice.



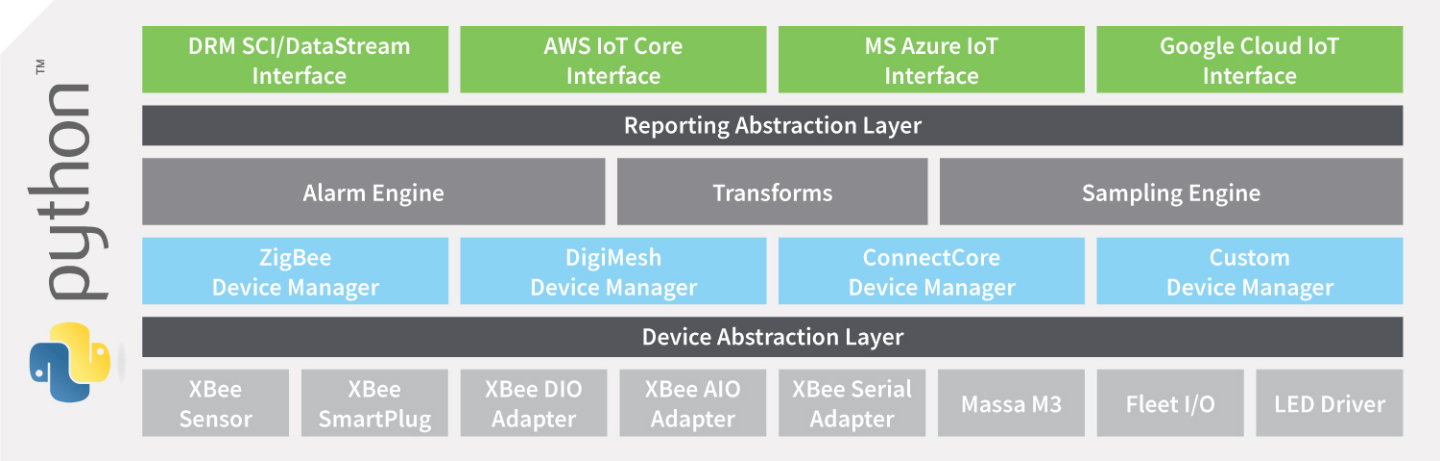
Managing integration complexity

To connect devices directly to the third-party IoT cloud provider, you can deploy business logic to your devices, such as Python code, that performs that function. Then you can easily push out software updates and configuration changes using the automated methods discussed earlier.

As another example, you can connect to a third-party application using the RESTful web services in DRM, and that application in turn has access to all the devices it is managing.

That can be accomplished in a few ways. One method is to pull the data or configure DRM to push data out to a listening application whenever new data arrives.

The device can also be programmed to connect directly to the third-party application. DRM is fundamentally agnostic, which means various kinds of business logic can be downloaded to those devices in order to transmit information from sensors, collect data or set functionality remotely. DRM always maintains that management connection to the devices so you are able to download new business logic if and when that is necessary.



Managing integration complexity with Python

For help planning your next IoT project, or to learn more about how to securely manage your IoT device deployment with sophisticated device management software, contact Digi today at www.digi.com/contactus.

Digi has many resources to support your IoT requirements.

IoT Development Resources

We can help with a wide range of development needs, including:

- Development of mobile or web applications
- Development of business logic to run in the Python interpreter on devices
- IoT implementation planning
- Certification support, from consulting to full design services with a guarantee that your design will pass certification the first time
- See the following pages for more information:
  - Digi Wireless Design Services
  - Digi Professional Services

IoT Monitoring and Management Resources

Digi offers a full range of tools and resources for managing IoT deployments.

- Digi Remore Manager: Securely monitor and manage your IoT device deployment
- Digi Security Center: Keep current with the latest updates on security threats and vulnerabilities
- Digi TrustFence: Ensure your deployment follows all best practices with Digi's security framework
- Digi Foundations™: Digi offers a complete package, including IoT hardware, DRM and expert support

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International
9350 Excelsior Blvd.
Suite 700
Hopkins, MN 55343

Digi International - Japan
+81-3-5428-0261

Digi International - Singapore
+65-6213-5380

Digi International - China
+88-21-5049-2199

Digi International - Germany

/digi.international @DigiDotCom /digi-international