# DigiCert® IoT Device Manager

digicert®

## Three common challenges

No matter the industry or the size of your organization, virtually every IoT initiative faces three major challenges when developing a secure ecosystem.

### 1. IoT without identity

You're only as secure as your most vulnerable connected device. But the more connections you add, the more difficult it becomes to recognize—much less remediate—potential weak points.

To build truly secure IoT, you first need a simple identity management tool that identifies, monitors and controls every device at every stage in the lifecycle.

### 2. Unmanageable complexity

Many IT infrastructures struggle with complex and siloed tech stacks, which are often the result of patching together different applications, vendors and services ad hoc as new demands and challenges arise.

As complexity grows, IT managers spend more time monitoring the different technologies than managing the security of the infrastructure as a whole.

What you really need is an integrated, start-to-finish solution that simplifies the complex in a single point of control.

### 3. Security without scalability

Around the world, IoT devices measure in the billions, and new ideas for connecting things are growing exponentially day by day. But no two IoT deployments are the same, which only complicates things, and regulations and security requirements are constantly evolving.

You need a flexible solution for rapidly deploying PKI services that fits your needs, and a platform that can keep pace with the increasing number and diversity of devices.

## One uncommon approach

DigiCert IoT Device Manager is built on DigiCert ONE, a new, modern PKI management platform designed to meet your unique needs—and meet the heavy demands of modern IoT deployments.

## Benefits

### Complete identity and control

Assign and manage device identity in large or small volumes at any stage of the lifecycle—from silicon injection to deployment in the field. Operate with total visibility over certificates issued to devices.

### Security and management—simplified

Manage discovery, reporting, dynamic certificate creation, revocation, user access and more. Create and provision custom certificate profiles to meet any needs—from devices as small as pacemakers to those as large as commercial airliners.

And, with automated backups, updates and load balancing, you'll enjoy optimal performance at scale without sacrificing speed or simplicity. All this, from a single, hyper-modern, user-friendly interface.

### Speed and flexibility

Set up and configure in a fraction of the time with a platform built for IoT. Automated ICA creation, powerful account options like flexible certificate profiles and templates, and a variety of protocol options with easy configuration make IoT Device Manager fast to stand up and simple to customize. Choose the deployment option that works best for your needs: DigiCert-hosted, on-prem, in your cloud, in-country or anywhere in between.

## Key features

- Manage the full device certificate lifecycle from creation and enrollment to provisioning, renewal, and revocation
- Generate standard and custom certificate profiles to meet the needs of any IoT deployment
- Permit issuing CAs to automate and quickly scale to large volumes of issuing CAs as needed
- Provision certificates at any stage—from secure chips to device assembly to the field
- Provision and track device identity
- Facilitate secure device updates
- Configure to fit your processes and compliance needs with containerized architecture
- Generate reports on certificate status, device identity and any other metadata
- Generate audit logs to ensure policy compliance

## Technical specifications

- Standard certificate management protocols include: SCEP, CMPv2, EST and ACME
- Flexible and customizable use of REST API including devices connecting directly to REST API for services and certificate provisioning and renewal
- HSM Support
  - Thales Luna Network HSM
  - Thales Luna G5
- Supported standards
  - OCSP and CRL certificate status
  - PKCS#10 certificate requests (CSR)
  - PKCS#12, PEM, and PKCS#7 certificate formats
- Services support 3GPP, LTE/4G/5G
- Communication over HTTP transport protocol

### Who is DigiCert?

The better way can't become common practice until someone finds it.

At DigiCert, building a better way to secure the internet is the single-minded pursuit that goes all the way back to our roots. That's why our TLS/SSL certificates are trusted everywhere, millions of times every day by 89% of the Fortune 500, 97 of the top 100 global banks, and for 81% of global e-commerce. It's why our customers consistently award us the most five-star service and support reviews in the industry. It's why we're modernizing PKI by building the DigiCert ONE platform and management tools to help enterprises and governments secure identities, access, servers, networks, email, code, signatures, documents and IoT devices. In SSL, IoT, PKI and beyond—DigiCert is the uncommon denominator.

Ready to learn more—or have questions about how DigiCert® can enable your individual initiative? Contact pki_info@digicert.com or call 1.801.770.1736 today.



digicert®