



Transforming the World through
the Power of Connectivity

New Relic | Electric Imp Workshop

August, 2016

Agenda

Electric Imp Company Overview

Collaboration Benefits of New Relic & Electric Imp

Workshop and Demo Overview

New Relic and Electric Imp integration:

Challenge 1: Tutorial

Challenge 2: Self-paced

Conclusion and Next Steps

Q&A



New Relic® &imp

Introduction to Electric Imp

Our Mission: Transform the world through the power of connectivity



Hugo Fiennes, CEO & Co-Founder

A history of leading development of world class connected device innovations



Led the hardware team through first four generations of Apple iPhone



nest

Designed and architected hardware for the Nest Thermostat



Founded 2011
HQ in Los Altos, CA
Product Development in the US and UK

Electric Imp Team: Experience across leading technology companies:



100+
customers

105+
countries

14 Billion

Messages processed per month

600,000+

Devices in the market

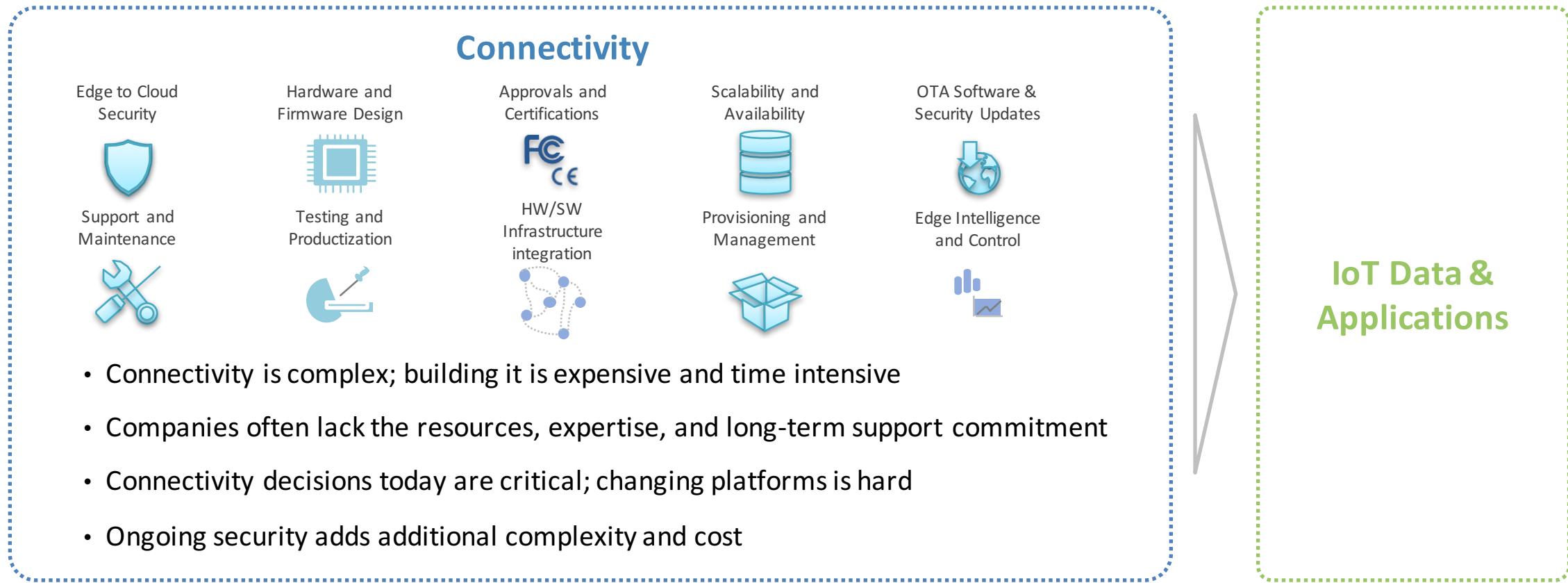
IoT Market Focus

Intelligent Buildings
Light Industrial

Energy
Connected Home Infrastructure

The Challenge of Connectivity

To realize the value of data, companies must first securely connect their products



Conclusion: To maximize ROI, companies should evaluate **Buy-vs-Build** for connectivity

Solution:

Electric Imp takes the Complexity out of Connectivity

Our leading IoT connectivity platform provides the core services to get any device online

Security

Ongoing, managed security-as-a-service for connectivity

Reliability

Less risk and reduced development costs with a proven platform

Flexibility

Easily adapt to different use cases & customer requirements

Scalability

Effortless scalability for large deployments

Seamlessness

Faster time to market with complete out-of-the-box connectivity and drop-in integration

The Electric Imp Connectivity Platform Components



Customer Proof Points

Our single platform meets the business objectives of a wide range of customers



**Connected Postage Meters
via "SmartLink"**

- Update units in the field
- Meet stringent security requirements
- Accommodate users with a wide range of technical aptitude



**Cybex "Care"
Connected Treadmill**

- Retrofit units in the field
- Provide predictive maintenance
- Expedite time to market



"The Shopping Button"

- Bridge between assets and the cloud
- Offer analytics for the real world
- Builds direct customer engagement



**"Bud-e Fridge"
Smart Home Beer Fridge**

- Automated fulfillment
- Usage tracking
- Accessible user experience
- Innovate brand engagement



**Vibration "mote" for
predictive maintenance**

- Retrofit industrial vibration monitoring
- Provide real-time analytics and dashboarding
- Reduce unplanned downtime and repair costs



Customers in a variety of roles use New Relic to solve problems faster and improve visibility.

DEVELOPERS

- Extra visibility helps them solve problems faster and build better apps.



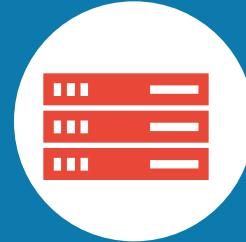
APPLICATION OWNERS

- Service-level responsibility to the business, understands monitoring from a transactional point of view.



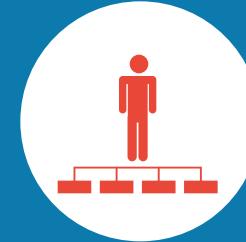
OPERATIONS

- Important to keep apps and services up and running. Availability and app health drives their business.



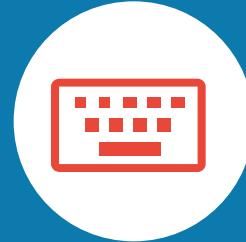
MANAGERS & EXECS

- Direct visibility into how performance is affecting the bottom line.



SUPPORT

- Quickly diagnose performance issues affecting customers. Reduce time to resolve issues.

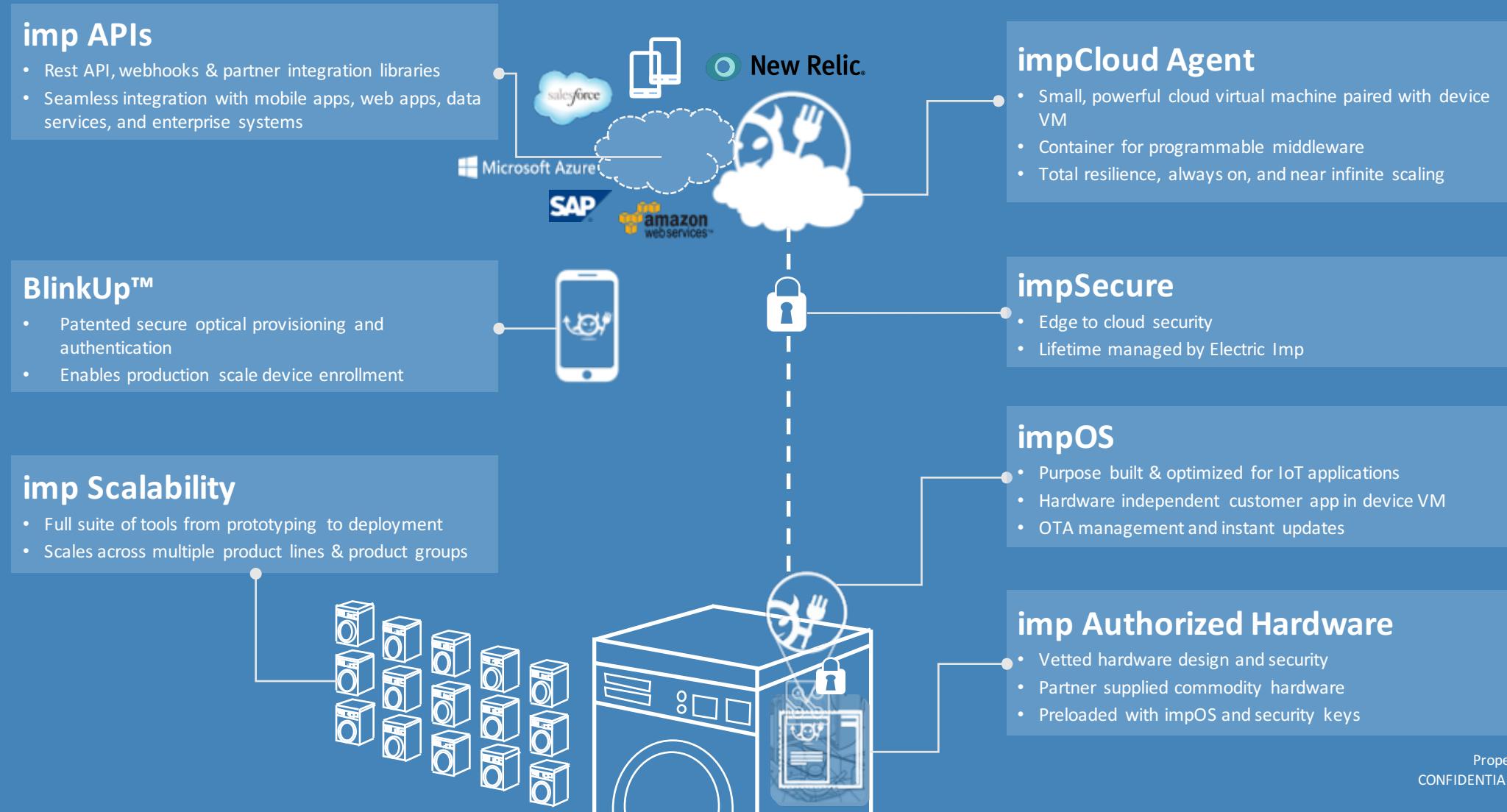




New Relic® &imp

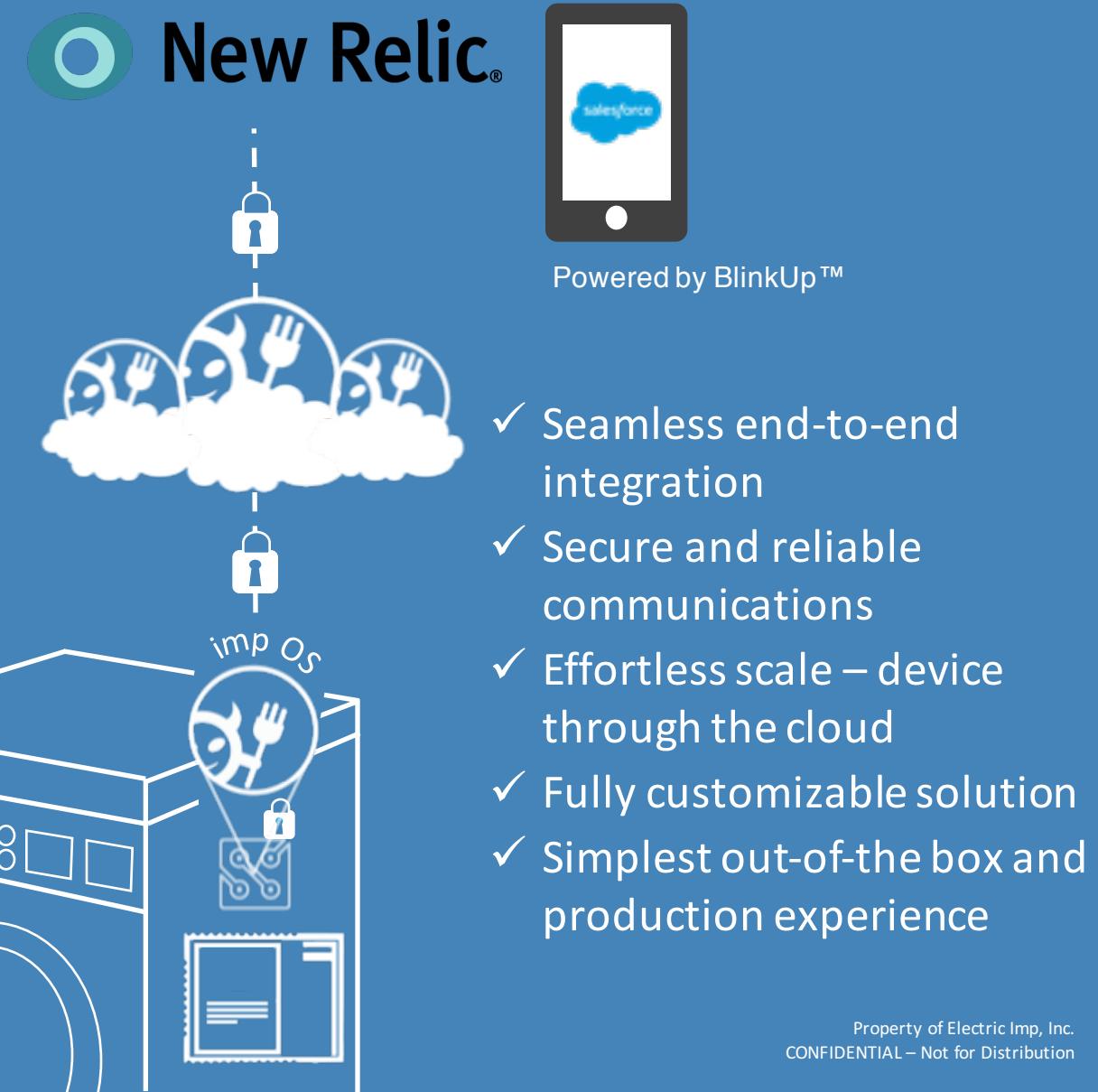
Collaboration Benefits

With Electric Imp's platform every device has a customizable, secure, powerful, and intelligent virtual presence



Why Electric Imp & New Relic?

- **Proven** edge-to-cloud solution to address real-world challenges of delivering, securing, and managing connected products
- **Low complexity**, IP-based architecture enables customers to easily connect devices to New Relic Insights and other services
- **Secure and scalable solution** allows easy customization and reuse across different use cases and products
- **Full visibility** of performance from the edge to critical backend systems



**Best-of-Breed
Device
Connectivity**

**Proven Security
for the Real
World**

**Delivering
Commercial
Products in
Volume since
2012**

**Unique Edge-to-
Cloud Virtual
Machine-based
Architecture**

**Ongoing
Platform
Security and
Maintenance
As-a-Service**

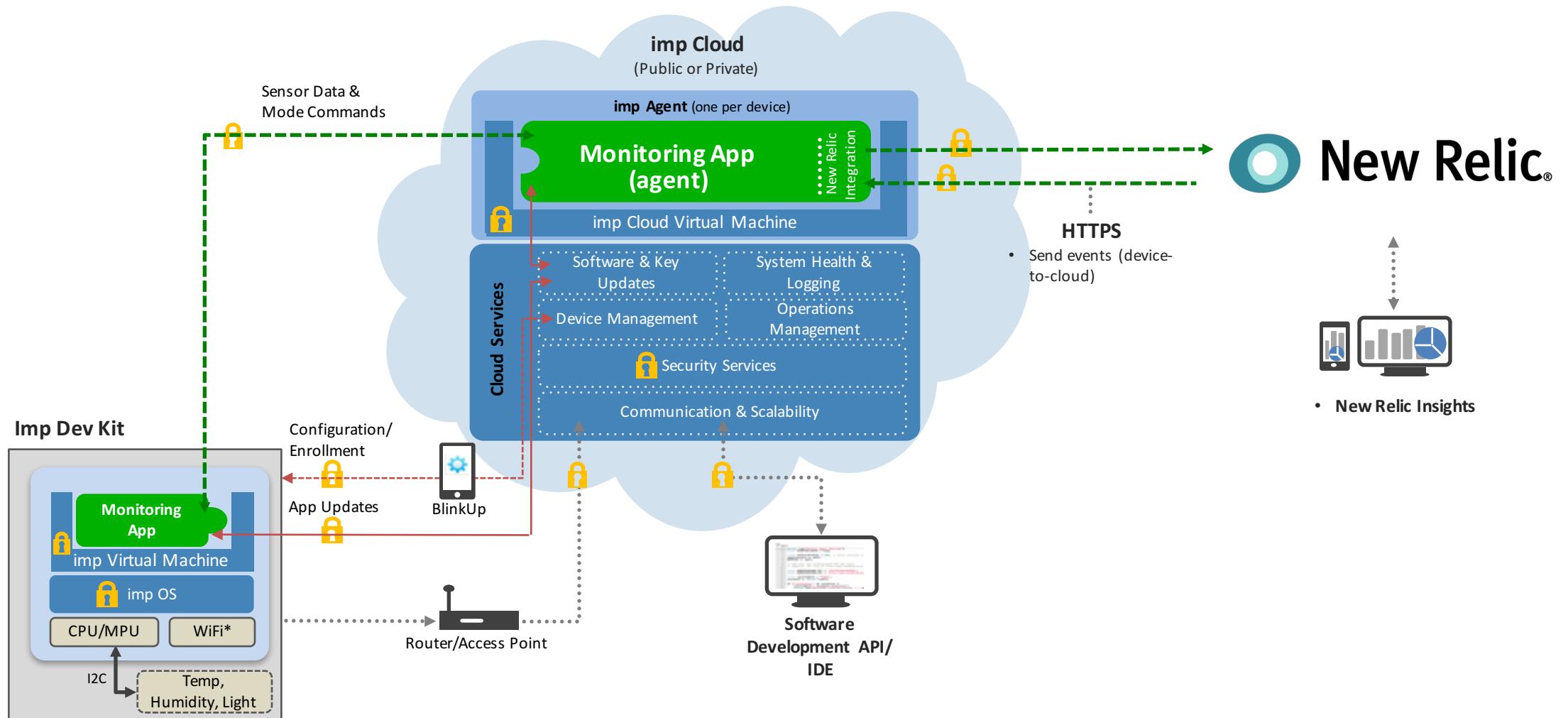
**Electric Imp is uniquely
positioned in the market to
address Enterprise IoT with
its technology, strategy and
leadership**



New Relic® &imp

Workshop & Demo Overview

Demo Architecture: Environmental Monitoring



Demo Application Structure

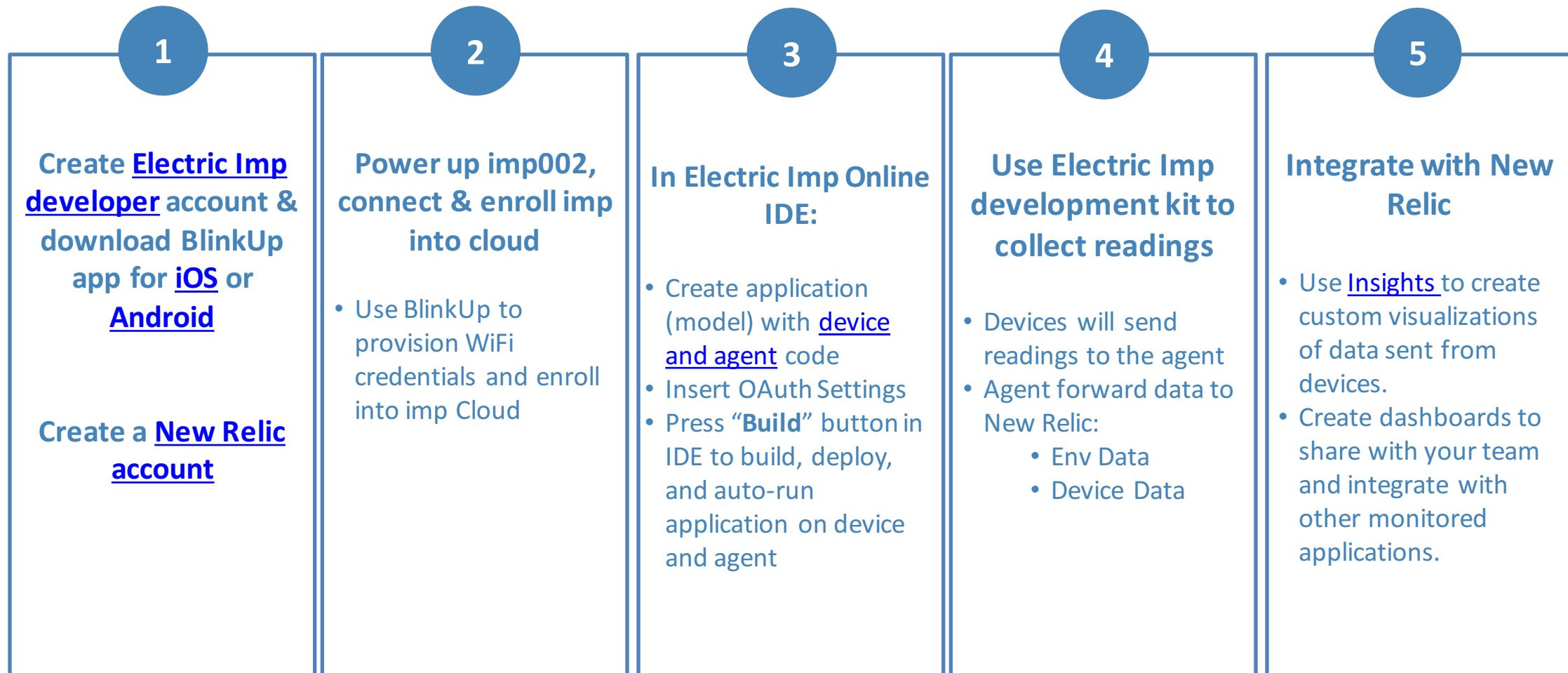
Device-side application

- imp002 Developer Kit + ‘Environmental Tail’
 - Single module Cortex-M4 MCU and WiFi
 - Temp + humidity sensors
- Monitor device and environmental conditions
 - WiFi strength, latency, free memory, and voltage
 - Temperature, humidity and light level
- Log readings
- Send readings to cloud agent

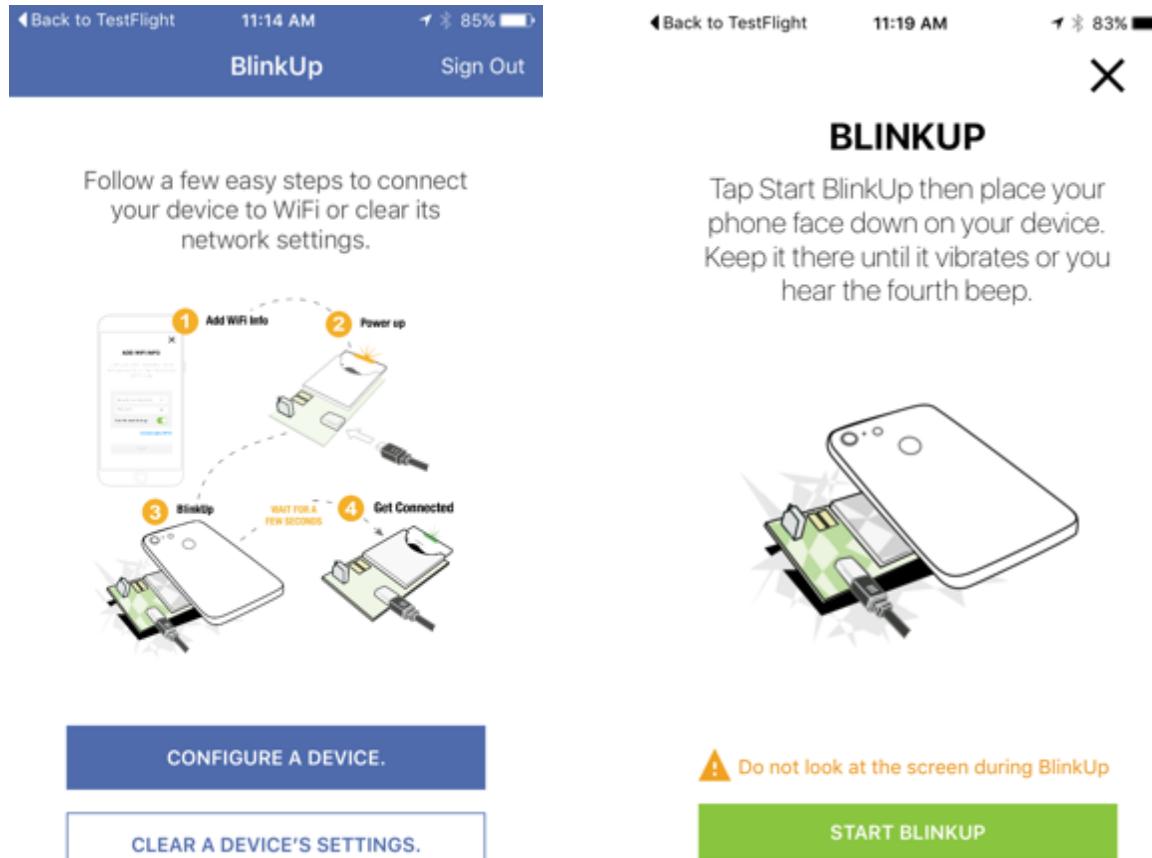
Cloud-side Agent application

- Endpoint for bidirectional device-agent communication
- Pass data between device and agent over secure, managed communication link
- Push data into New Relic
 - Temperature, humidity and light level
 - WiFi strength, free device memory, message round-trip time

Demo Overview and Steps



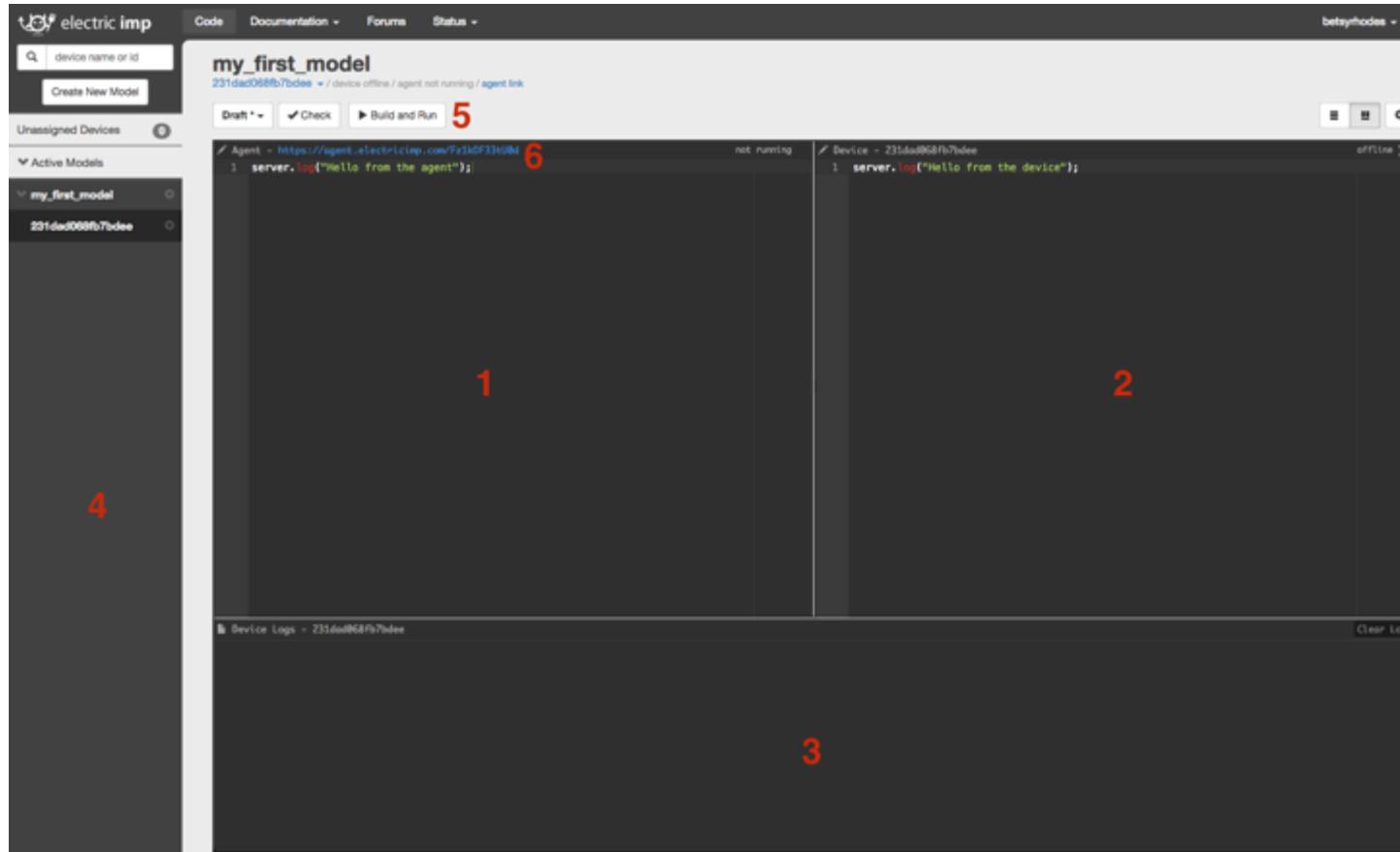
Electric Imp App/BlinkUp™: Simple and secure method of provisioning a device to end user Wi-Fi network



- Mobile app uses light pulses to pass information (SSID & password) to the device
- Device is automatically authenticated, enrolled into the Electric Imp cloud, and provisioned (e.g. Wi-Fi network)
- Now you can program your device in the online IDE

IDE Overview

ide.electricimp.com

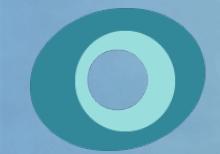


- 1 – Agent Code Window
- 2 – Device Code Window
- 3 – Log Window
- 4 – Sidebar
 - Models
 - Devices
- 5 – Build and Run
- 6 – Agent URL



&imp

Electric Imp IDE Demo



New Relic® &imp

Challenge 1 (tutorial)

Reminder: You need these things to continue...

- You should already have set up your Electric Imp Account and blinked up your Imp
- A New Relic account

New Relic Account Settings

rpm.newrelic.com/accounts

The screenshot shows the New Relic account settings interface. A red box labeled '1' highlights the 'Account settings' link in the top right corner of the sidebar. A red box labeled '2' highlights the 'INTEGRATIONS' section in the sidebar, with 'API keys' selected. A red box labeled '3' highlights the 'Your account ID is: 1210987' message. A red box labeled '4' highlights the 'Insights API keys' section under 'Other keys'.

Integrations for: Electric Imp_7

ACCOUNT

- Summary
- Subscription
- Usage
- Billing

SECURITY AND AUTHENTICATION

- High security
- Single sign-on
- Session configuration

INTEGRATIONS

- API keys** (highlighted by a red box)
- API Explorer
- Data sharing
- Alerting notifications
- Ticketing integrations
- Add integrations

PARTNERSHIPS

- Partnerships

ESTABLISHED RELEASES

- Java
- .NET

CONNECTED AGENTS

API keys

Integrate your data

New Relic's REST API makes it easy to connect your monitoring data and configurations to your code, your systems, and your business.

Key: (Show key)

NOTE: We disabled the ability to change the API key in the UI for New Relic NR

Regenerate REST API key | Delete REST API key

Other keys

New Relic license key

Insights API keys (highlighted by a red box)

Data access key - deprecated

Your account ID is: 1210987 (highlighted by a red box)

Admin user's API keys

User	Admin's API key	Date last used	Action
Admin	-	-	Regenerate
Elizabeth Rhodes	-	-	Regenerate
Terrence Barr	-	-	Regenerate

Regenerate all

- 1 – Account Settings
- 2 – Integrations ->
- API keys
- 3 – Note Your Account ID
- 4 – Click Insights API keys

New Relic API Key

insights.newrelic.com/accounts

The screenshot shows the New Relic Insights API Keys page. On the left, there's a sidebar with various links like 'Query', 'Data Explorer', 'Data apps', 'Create a dashboard', 'Manage data', 'Documentation', and 'Support forum'. Below that are download links for the App Store and Google Play.

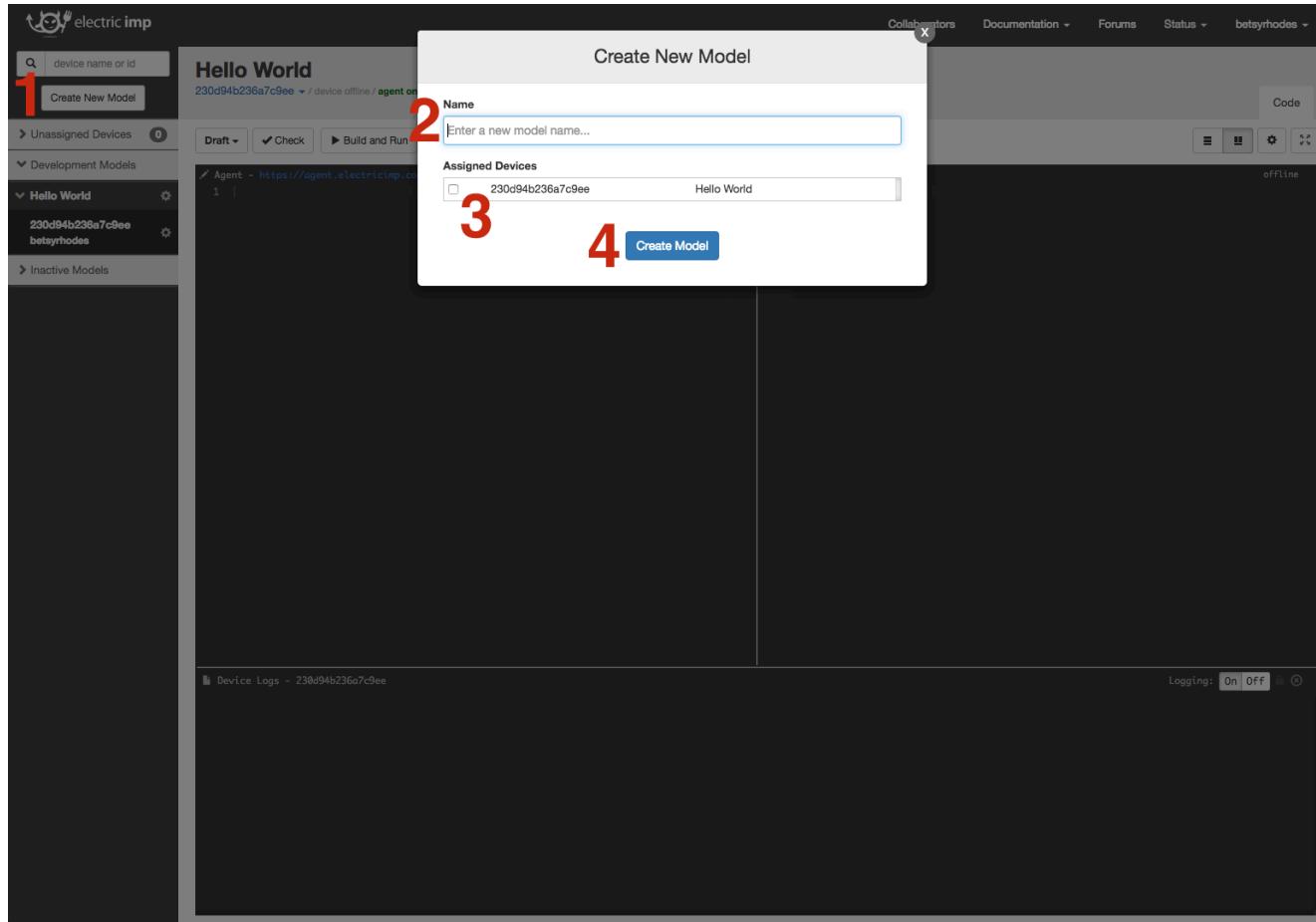
The main content area has two sections:

- Insert Keys**: Contains documentation and a curl command example. A red box highlights the 'Key' field, which contains the value: `vF713R87rGeY9-eonB9Ez_UjKfIDHxx`.
- Query Keys**: Contains documentation and a curl command example.

- 1 – Click Show
- 2 – Note Your API Key
- Note: this is an Insights key, not the REST API Key.

Electric Imp Create New Model

ide.electricimp.com



- 1 – Click Create New Model
- 2 – Enter Name for your Model
- 3 – Assign your Device to the Model
- 4 – Click Create Model

Electric Imp Run Example Code

ide.electricimp.com

New Relic Workshop Example
230d94b236a7c9ee / device offline / agent online / agent link

Draft ✓ Check ▶ Build and Run 4

Collaborators Documentation Forums Status betsyrhodes

Unassigned Devices 0

Development Models

New Relic Workshop Example 1
230d94b236a7c9ee betsyrhodes 2

Inactive Models

Agent - https://agent.electricimp.com/b3rf97on8yol

```
const ACCOUNT_NUMBER = "<YOUR-ACCOUNT-NUMBER-HERE>";
const API_KEY = "<YOUR-API-KEY-HERE>";

// Asynchronous request
device.on("envlog", function(data) {
  local insightsData = {
    "ts" : time(),
    "devId" : data.devId,
    "temp" : data.temp,
    "humidity" : data.humid
  };
  server.log("---- envdata ----");
  server.log("ts: " + insightsData.ts);
  server.log("devId: " + insightsData.devId);
  server.log("temp: " + insightsData.temp);
  server.log("humidity: " + insightsData.humidity);

  // Send asynchronously
  insights.sendEvent("envdata", insightsData, function(err, result) {
    // If there was an issue, report it
    if (err != null) {
      server.error(err);
      return;
    }
    // Otherwise, log success
    // server.log("Success");
  });
});

device.on("applog", function(data) {
  local insightsData = {
    "ts" : time(),
    "devId" : data.devId,
    "lightLevel" : data.lightLevel,
    "freeMem" : data.freeMem,
    "wifisignal" : data.wifisignal,
    "rtt" : data.rtt
  };
  server.log("*** appdata ***");
});

// Device - 230d94b236a7c9ee
1 #require "S1702x.class.nut:1.0.0"
2 devId <- hardware.getdeviceId();
3 millis <- 0;
4 rtt <- 0;

5 // Initialize I2C and sensor
6 hardware.i2cB99.configure(CLOCK_SPEED_400_KHZ);
7 tempHumid <- S1702x(hardware.i2cB99);

8 // Configure LED
9 ledPin <- hardware.pin2;
10 ledPin.configure(DIGITAL_OUT, 0);

11 // Heartbeat blink
12 function blinkHeartbeat() {
13   ledPin.write(1);
14   imp.sleep(0.5);
15   ledPin.write(0);
16 }

17 function testRoundtrip() {
18   imp.request("testRoundtrip");
19   millis <- hardware.millis();
20   agent.send("ping", 0);
21 }

22 agent.on("pong", function(data) {
23   rtt = hardware.millis() - millis;
24 });

25 agent.on("pong", function(data) {
26   rtt = hardware.millis() - millis;
27 });

28 // Periodically get env data
29 function logEnvData() {
30   imp.wakeup(1, logEnvData); // schedule next call
31 }

32 tempHumid.read(function(result) {
33   if ("err" in result) {
34     server.error(result.err);
35     return;
36   }
37   blinkHeartbeat();
38 }

39 //***** Logging *****
40 local envLogData = {};
41 envLogData.devId <- devId;
42 envLogData.temp <- format("%.1f", result.temperature).toFloat();
43 envLogData.humid <- format("%.0f", result.humidity).toFloat();

44
45
46
47
48
```

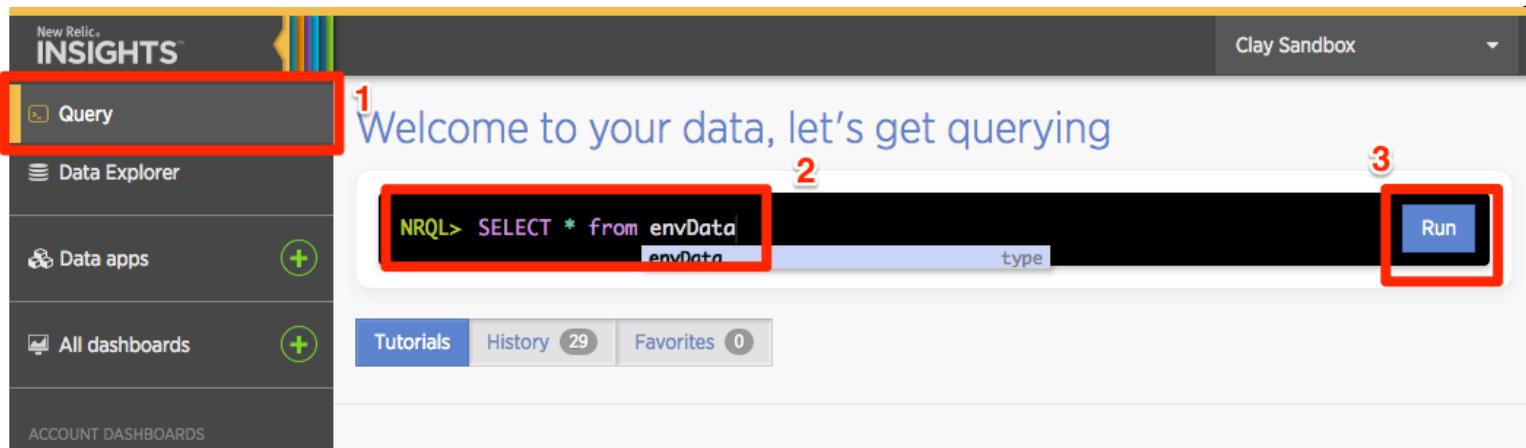
Device Logs - 230d94b236a7c9ee

Logging: On | Off

- 1 – Copy and Paste Agent Code
[EnvironmentalMonitoringExample.agent.nut](#)
- 2 – Copy and Paste Device Code
[EnvironmentalMonitoringExample.device.nut](#)
- 3 – Enter Your New Relic Info
 - Account Number
 - API Key
- 4 – Click Build and Run

Your first NRQL query

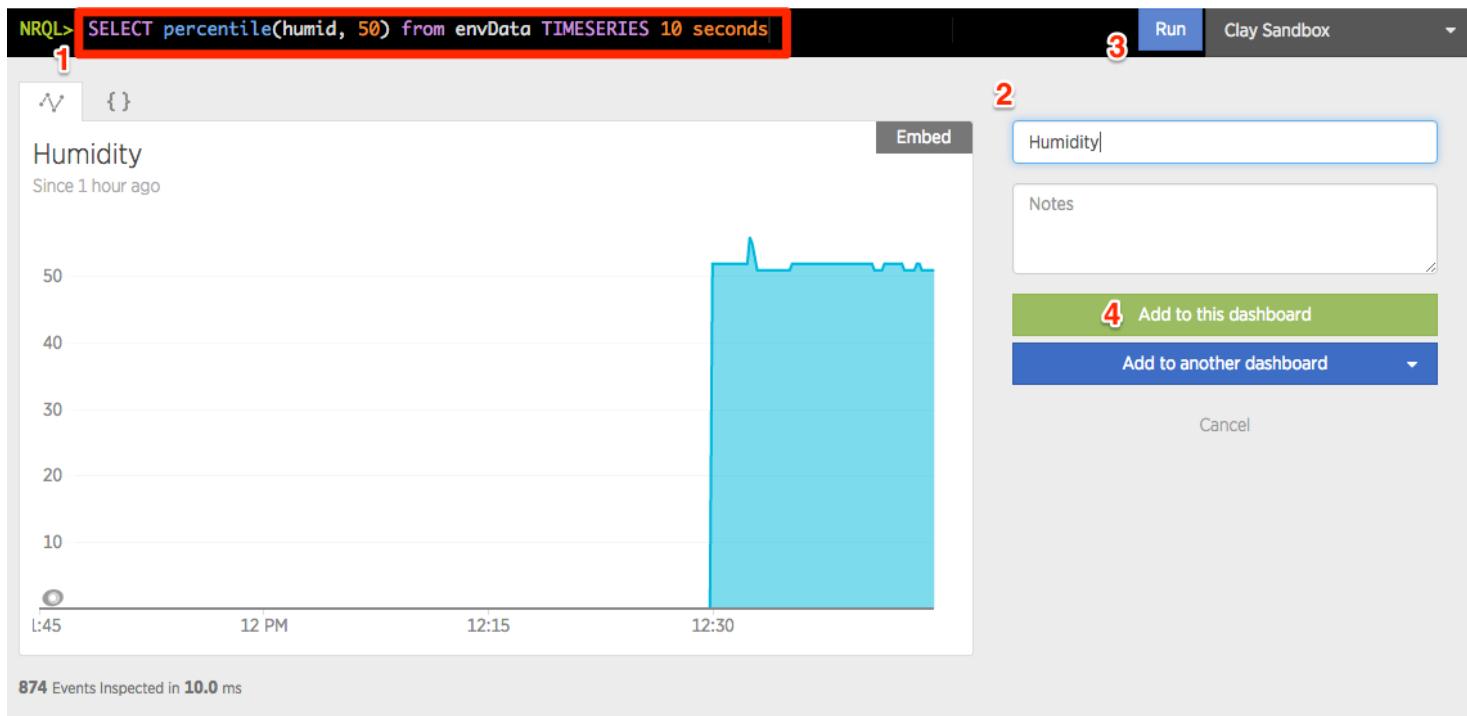
<https://insights.newrelic.com>



- 1 – Click “Query”
- 2 – Enter “SELECT * from envData” (just like SQL!)
- 3 – Click “Run” to execute query and see results being sent to Insights.

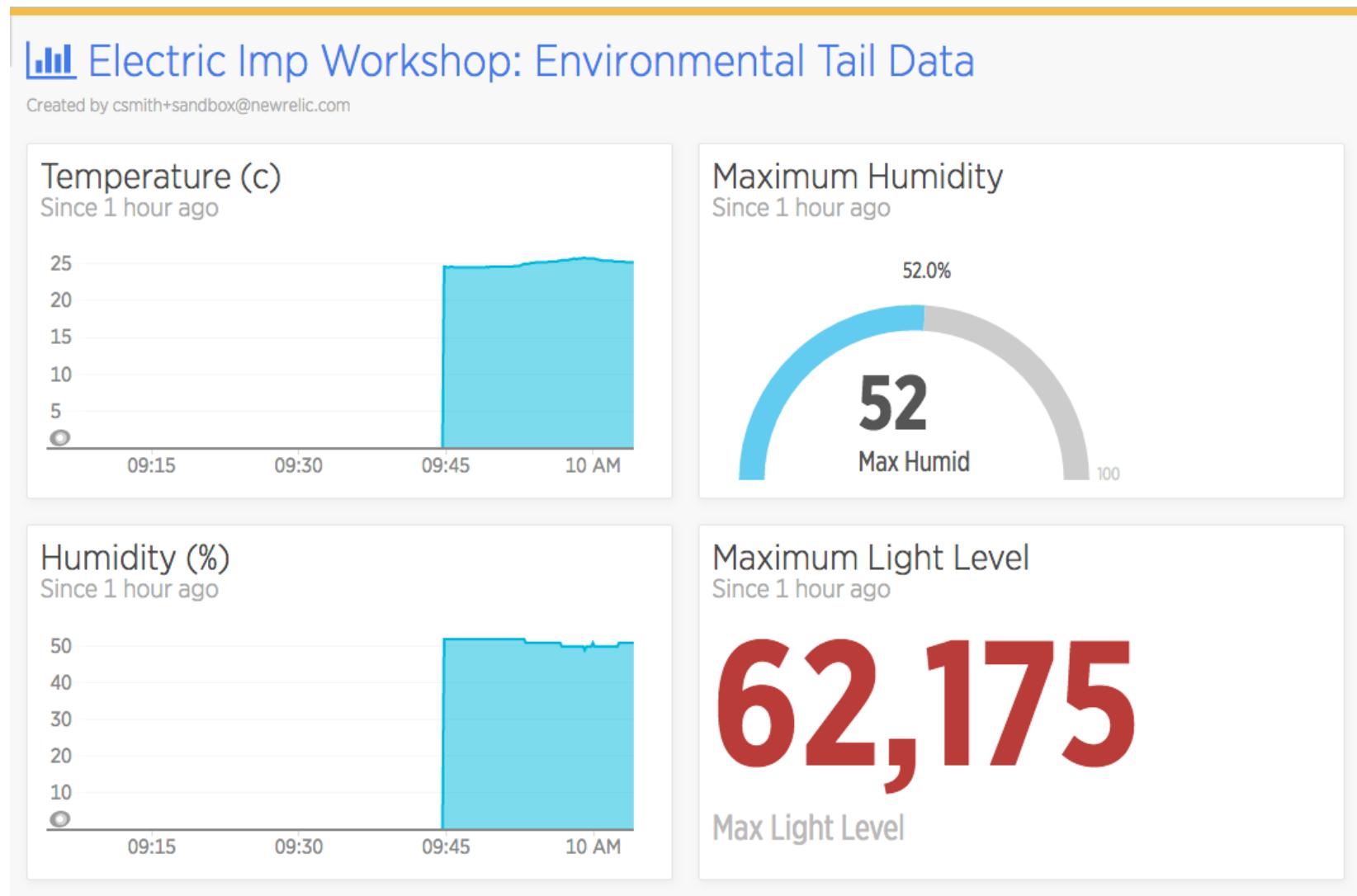
Visualizing Humidity Readings

<https://insights.newrelic.com>



- 1 – Write a query to visualize data
- 2 – Give the chart a title
- 3 – Click “Run” to execute query
- 4 – Add to your dashboard

Experiment with Queries and Add New Widgets





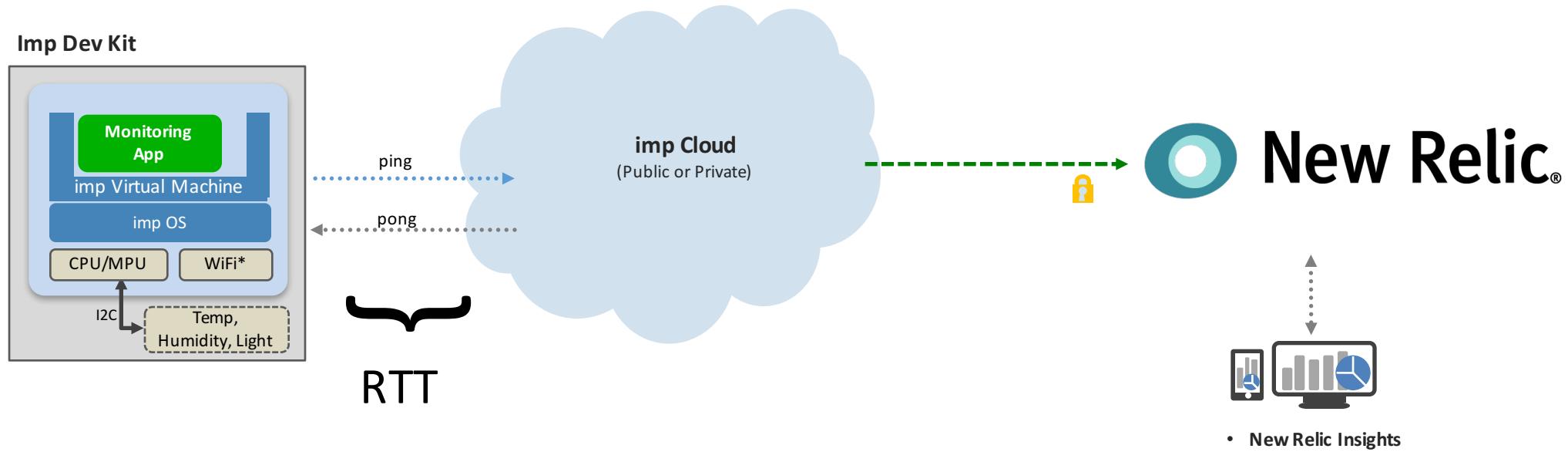
New Relic® &imp

Challenge 2 (self-paced)

Challenge 2: Monitoring Application Performance at the Edge

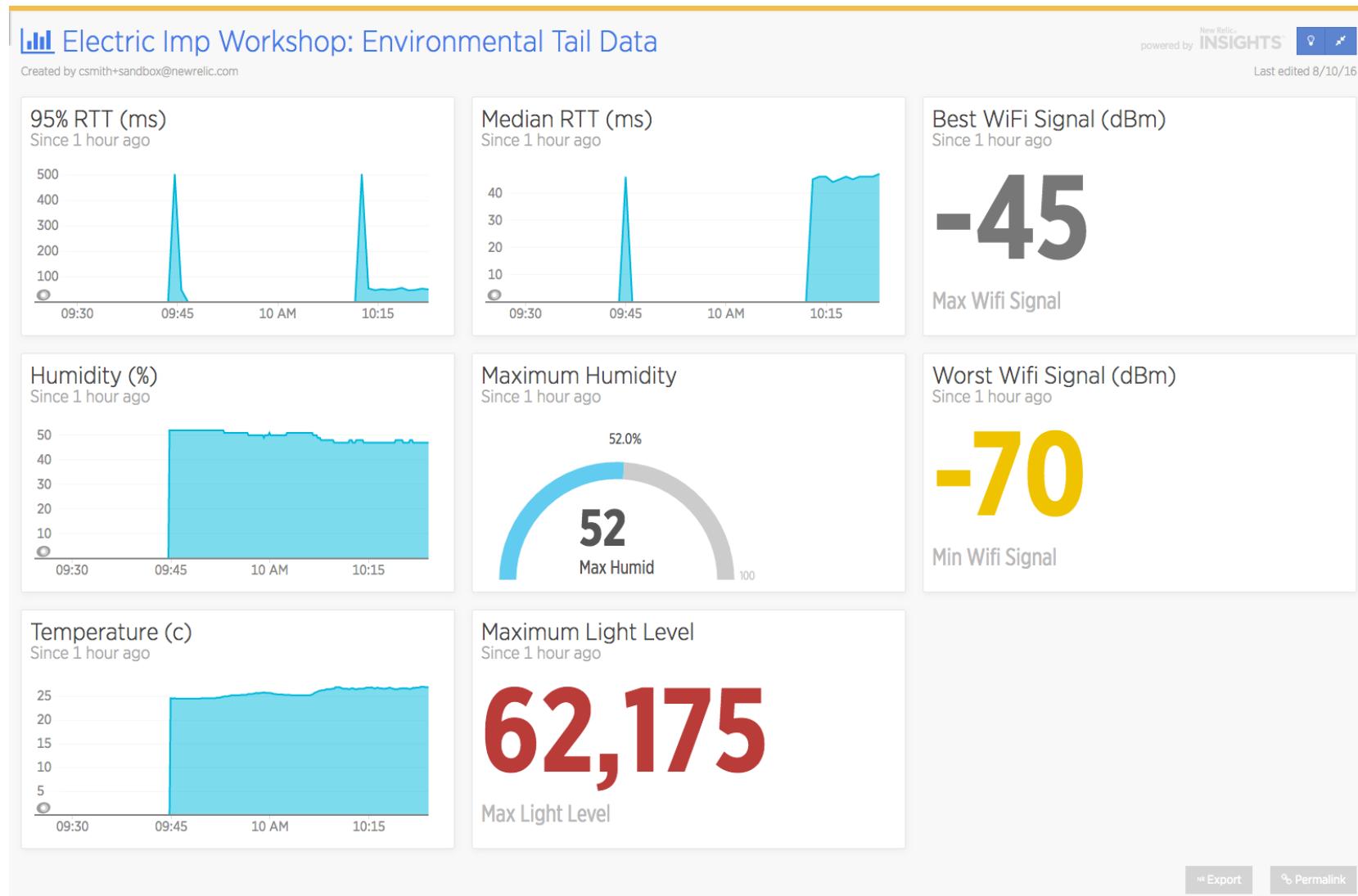
- Previous Challenge: Monitor environmental parameters
- This Challenge: Monitor the edge application itself
 - Capture key performance metrics indicative of application/device performance
 - Send to New Relic Insights
 - Analyze metrics, generate statistics, provide insights into application performance at the edge
- Suggested metrics to monitor
 - Device WiFi signal strength
 - Free application memory
 - Message communication round-trip time
- Hints:
 - See <https://electricimp.com/docs/api/hardware/> and <https://electricimp.com/docs/api/imp/>
 - To measure round-trip time, use agent.send()/agent.on() ping-pong
 - As data gets send to Insights, create new dashboards that display results.
<https://docs.newrelic.com/docs/insights/new-relic-insights/using-new-relic-query-language/using-nrql>

Measuring Round-Trip Time (RTT) for Better Network Visibility



- Goal: understand the impact of network latency from the Imp to the cloud
- Implement simple “ping/pong” event that measures time elapsed, send to New Relic
- **Don’t blame the network:** understand how it impacts performance

Recap: Complete Dashboard Example



&imp

Conclusion and Next Steps

Conclusion and Next Steps

Electric Imp & New Relic: A Extending Application Monitoring to the Edge

- Easy device integration into New Relic Insights (and other New Relic services, TBC)
- Our integrated product offering can rapidly enable high value end-to-end IoT solutions
- We focus on the complexities of device connectivity and security so you can focus on your value-add

Next Steps

- Integrate imp monitoring with existing backend software monitored by New Relic for full visibility from the edge to internal systems
- Use data to diagnose performance issues and discover connectivity issues or errors
- Know how your IoT devices are performing on different networks



New Relic® &imp

Q&A

&imp

Transforming the World Through
the Power of Connectivity

padma@electricimp.com

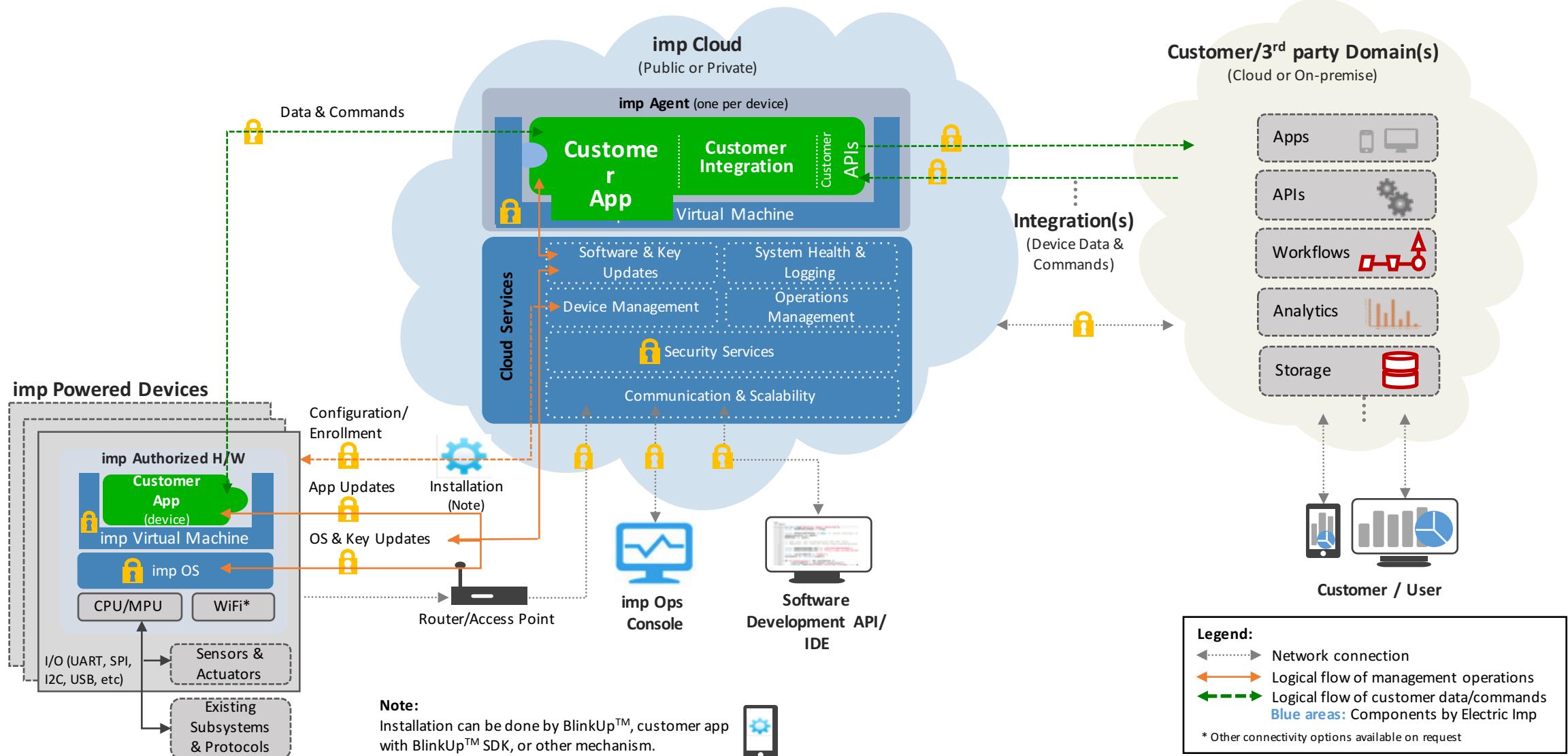
www.electricimp.com



New Relic® &imp

Appendix: Technical Deep Dive

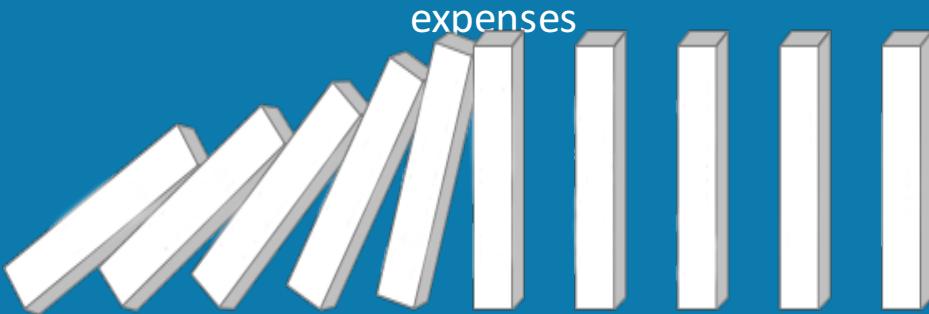
Electric Imp Platform Architecture Overview



Electric Imp provides Worry-Free Security

Security is considered the number one inhibitor to IoT implementations

A security breach from just one device can cost a company millions of dollars in revenue loss, brand damage and expenses



To safeguard the IoT, security must be designed in from the

The Electric Imp platform has an unparalleled security architecture from the hardware through the cloud

- **Device Security** - Hardware keys and code protected within the silicon
- **Communications Security** - Industry standard TLS link security and forward secrecy
- **Local Network Security** - Real activity is masked by random traffic
- **Device <>> Server Monitoring** - Server and device identities are confirmed before any communication
- **Cloud Server Security** - Network servers firewalled and only accessed through a secure protocol
- **Secure Remote Updates** - Devices are updated automatically and seamlessly

Security is designed in to every level of our platform's architecture

We use industry standards and best practices throughout the product's lifetime

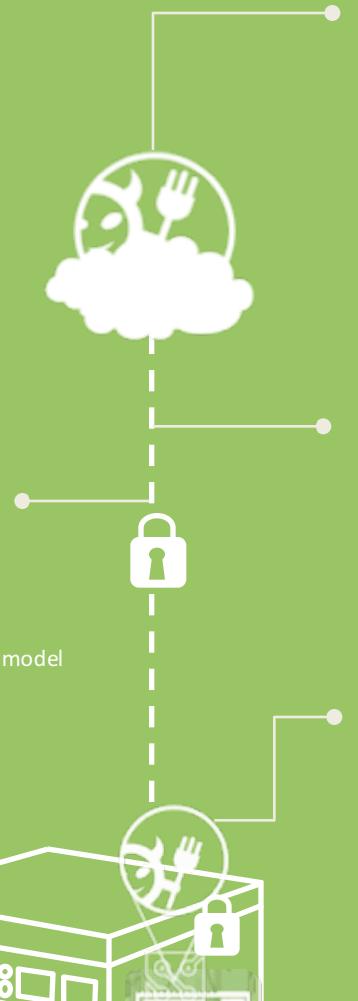


Provisioning

- Replay-proof token-based optical provisioning system uniquely identifies user & device
- Simple: increases chances of being done correctly

Application

- Application storage either on-die or AES-GCM encrypted depending on model
- Secure OTA upgrades via TLS channel to server
- TOTP authorized deployments*



Servers

- Device link crypto terminated on home server (running agent), not load balancer
- Servers reside within VPC, minimal open ports
- Full PKI chain validation for outbound HTTPS connections from agent (vs on device which wouldn't have resources)
- Standard best practices including use of bastion host, minimal privileges, etc.
- Automated monitoring and configuration management of clusters

Link

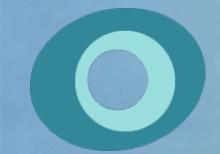
- Minimal attack surface (no open ports except DHCP & DNS)
- Industry standard TLS 1.2 protected link, with forward secrecy (ephemeral DH)
- Parties validate each other with RSA certificates
- AES-128 or 256 encryption
- Outbound connection from device to cloud - no firewall holes
- Secondary non-impersonation protection using ECC challenge-response
- Random link maintenance traffic to hide application traffic patterns

OS

- OS, network & security stack is maintained independently of application by Electric Imp for all devices
- OS updates do not require application involvement
- OTA OS upgrades/key management protected by RSA signing & AES-GCM encryption
- HSM-protected OS signing keys

Hardware

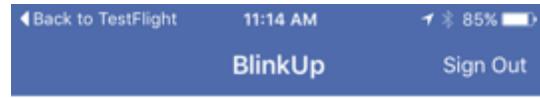
- Secure boot, debug interfaces permanently disabled
- Unique per-device keys provisioned at time of module manufacture
- All off-die storage AES-GCM+AEAD encrypted with per-device keys
- Hardware no-execute protection on all writable RAM (violations reported to server over TLS)



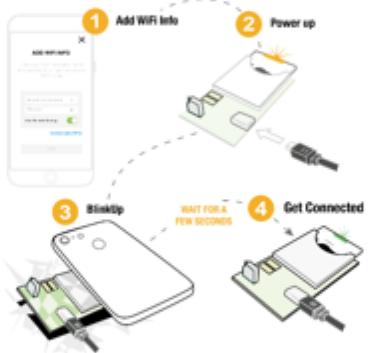
New Relic® &imp

Appendix: Electric Imp
Getting Started Guide

BlinkUp™



Follow a few easy steps to connect your device to WiFi or clear its network settings.



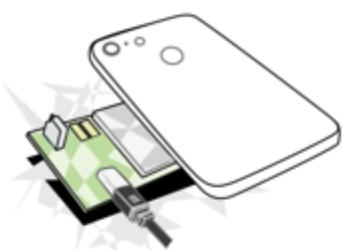
CONFIGURE A DEVICE.

CLEAR A DEVICE'S SETTINGS.

Signed in as: uxprod



Tap Start BlinkUp then place your phone face down on your device. Keep it there until it vibrates or you hear the fourth beep.



⚠ Do not look at the screen during BlinkUp

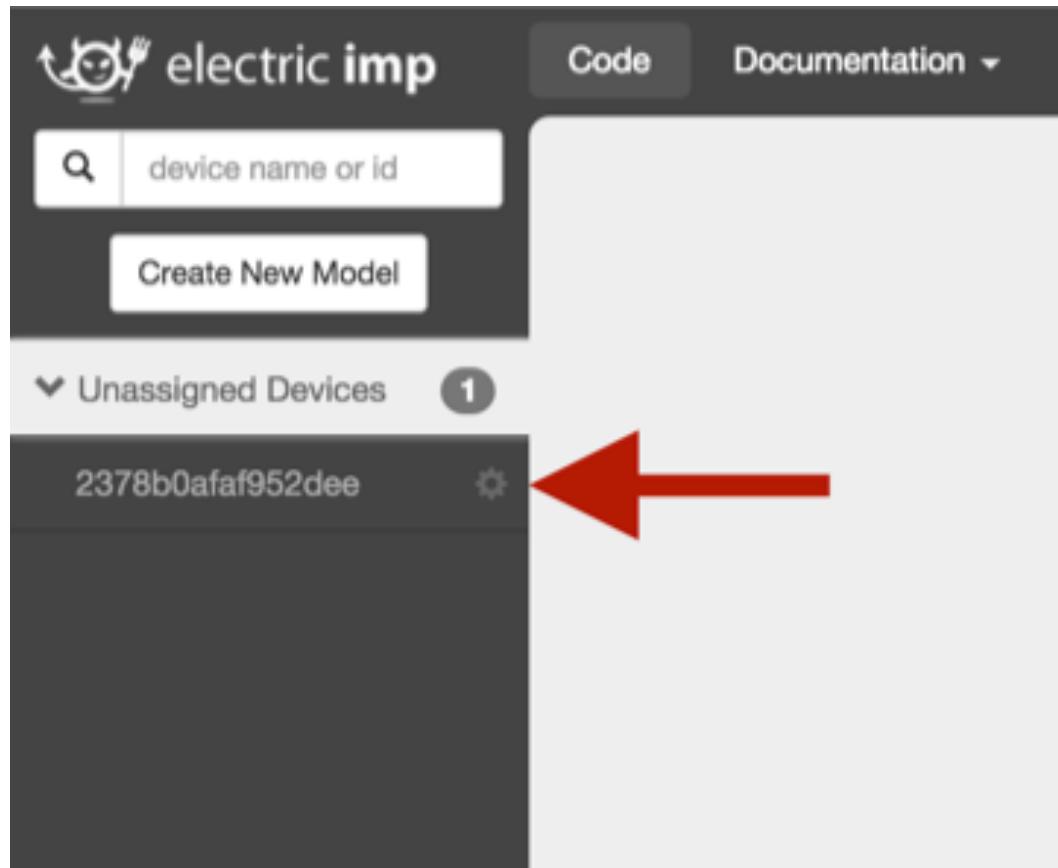
START BLINKUP



- Sign into the Electric Imp app
 - Click "**CONFIGURE A DEVICE**"
 - Enter your WiFi credentials, then click "**NEXT**"
 - Power up your imp with the USB cable, then click "**NEXT**"
 - Click "**START BLINKUP**"
- Cover the imp with your phone until BlinkUp completes
- Your device should now be blinking green (online)
- If you have any trouble visit [BlinkUp Troubleshooting Guide](#)

Create a new model

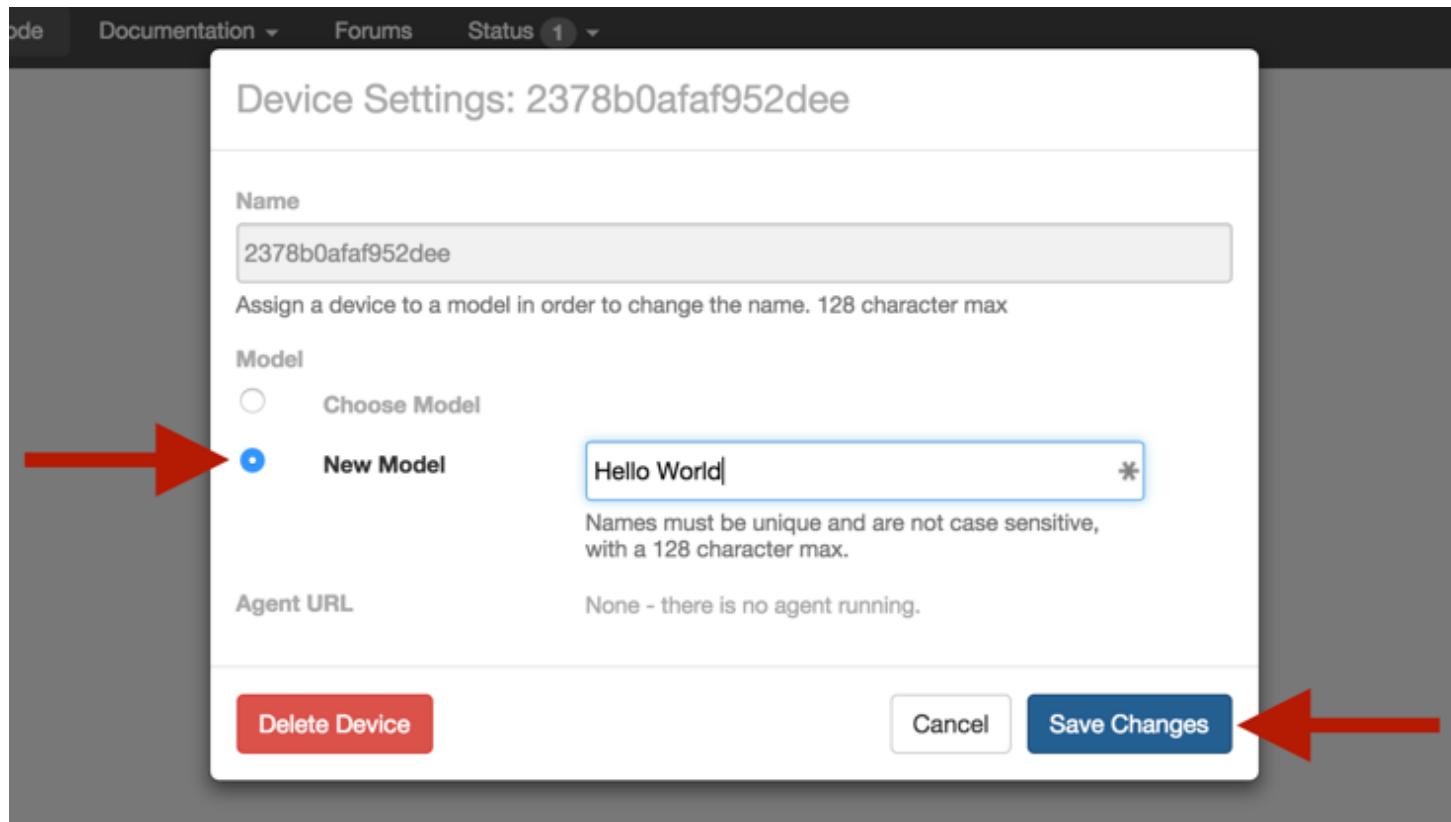
ide.electricimp.com



- - Open the IDE
- - Find your unassigned device
- - Click the Device Settings Gear

Create a new model

ide.electricimp.com



- Select "New Model"
- Enter a Model Name
- Click "Save Changes"