



TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT

Using Secure Connector for IoT

Best practice

Agenda

- Use SC to connect your IoT device to Azure
- SC LXC container
- Edge intelligence with NodeRed
- Tips and tricks



MXChip DevKit



MXChip DevKit

IoT DevKit

Get Started Docs Projects Blog v1.6.2

PROJECTS CATALOG

HOW-TO GUIDES

- Firmware upgrading
- Use configure mode
- Understand security chip
- Disable data collection

FAQ


API REFERENCE

- Arduino
- AudioV2
- Display
- EEPROMInterface
- FileSystem
- HTTP Client
- External Interrupts
- IrDA
- LED
- MemoryPool
- Memory Status
- Mutex
- OTA Programming
- Queue
- Semaphore
- Sensor: Humidity & Temperature (HTS221)
- Sensor: Magnetic (LIS2MDL)
- Sensor: Pressure (LPS22HB)

Project Catalog


Official tutorials that guide you build and learn IoT empowered by Azure.

EASY




Get Started

Send sensor data from DevKit to Azure IoT Hub.




MEDIUM




Firmware OTA

Update IoT DevKit firmware OTA (Over-the-Air) through Azure IoT Hub Automatic Device Management.




EASY



Connect to Microsoft IoT Central

Learn as a device developer, to connect a DevKit to your Microsoft IoT Central application. All within 5 minutes.


EASY



Remote Monitoring

Visualize sensors status on IoT DevKit using Azure IoT Remote Monitoring solution accelerator

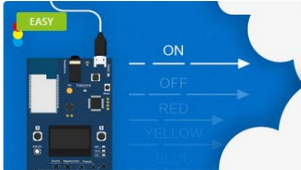
MEDIUM



Device registration with DPS

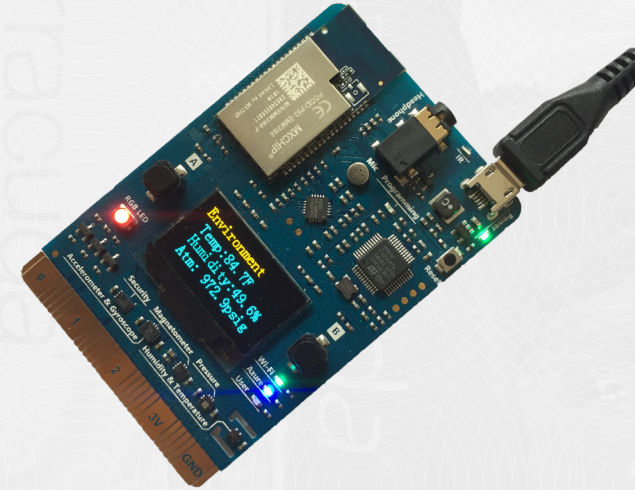
Use the Device Provisioning Service to automatically provision security enabled devices to IoT hub

EASY



DevKit State

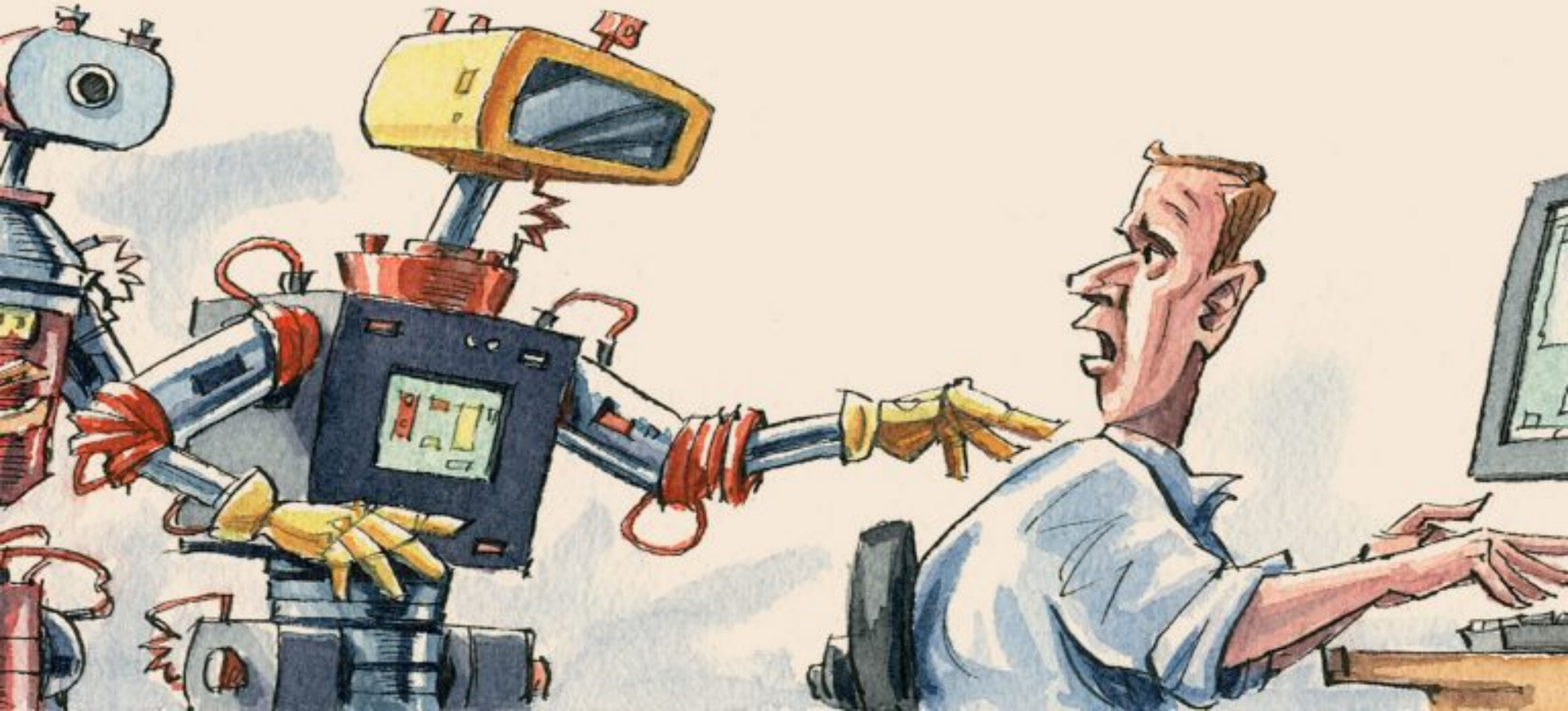
Monitor DevKit states and control the user LED with Azure IoT Hub device twins.



Edge computing



What do we expect?



Cross platform challenges



```
{"deviceId": "Device1",  
"SAK": „supersecureaccesskey”,  
"Protocol": "mqtt",  
"Data": { „Temp": "25" }}
```



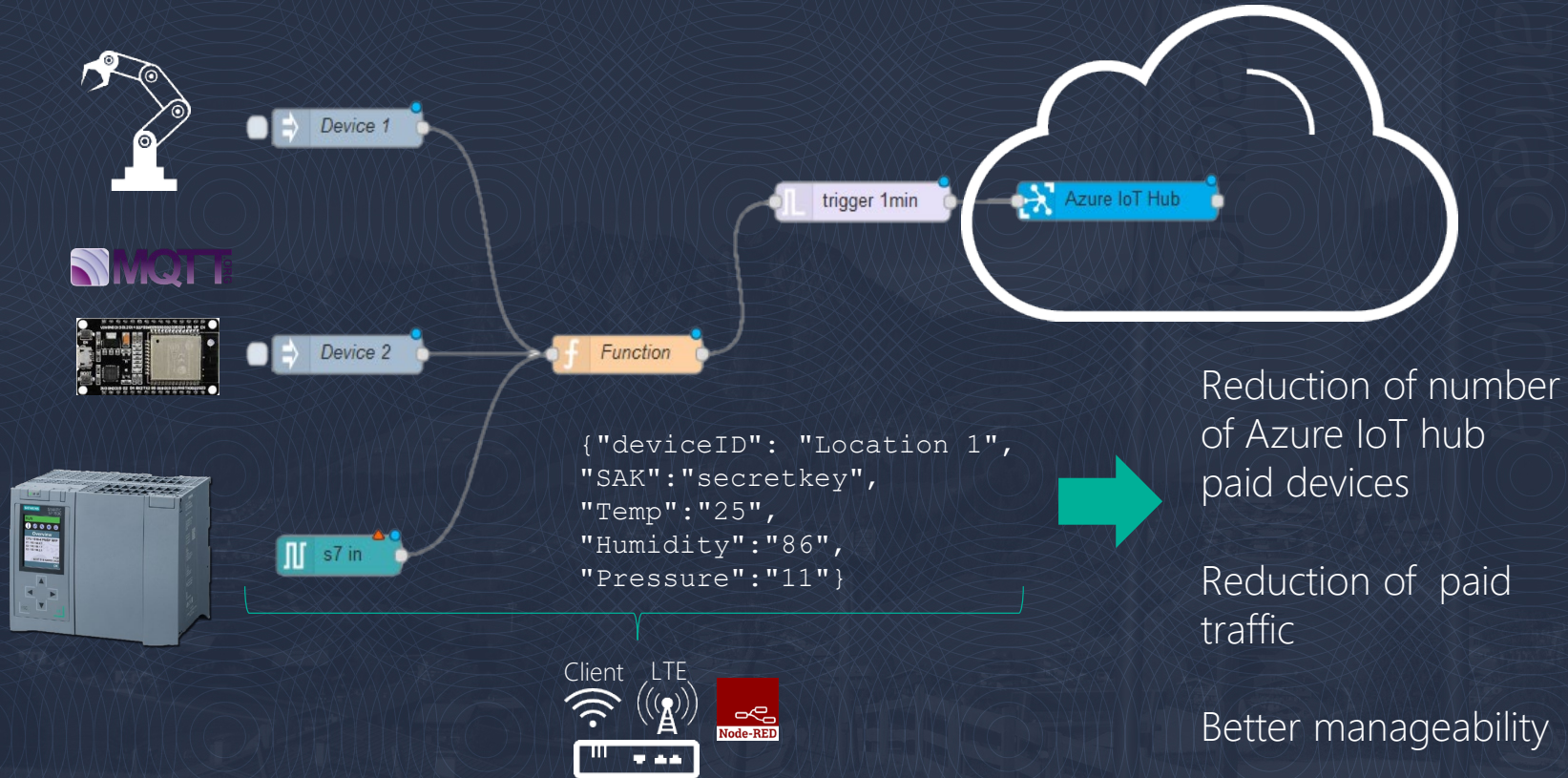
```
{"deviceId": "Device2",  
"SAK": „supersecureaccesskey1”,  
"Protocol": "mqtt",  
"Data": { „Humidity": „58" }}
```



```
{"deviceId": "Device3",  
"SAK": „supersecureaccesskey3”,  
"Protocol": "mqtt",  
"Data": { „Pressure": „11" }}
```



Data reduction & Control consolidation



Live Demo



More performance is on the way!



SC2 2 cores @ 1GHz (1 core)

1 GB RAM (512 MB)

16 GB storage (2 GB)



SC3 4 cores @ 1.2GHz

2 GB RAM

16 GB storage + 8 GB internal



Tips and tricks



Epoch

00000000 00000000 00000010 01100000

```
root@SMPq:~# date  
Thu Jan  1 00:10:10 UTC 1970
```



Internet is not Internet

Barracuda Firewall Admin 8.0 - root @ wmlB - Firewall / Live

51.145.148.47 wmlB

DASHBOARD CONFIGURATION CONTROL FIREWALL VPN LOGS STATISTICS EVENTS SSH

Monitor Live History Threat Scan Audit Log Shaping Users Dynamic Host Rules Forwarding Rules Sync Filter 5 Sessions Refresh Always

Traffic Selection Forward, Local In, Local Out, IPv4, IPv6 **Status Selection** Closing, Established, Failing, Pending **Source** 192.168.0.11

ID	State	IP Protocol	Port	Source	Interface	User	Destination	Protocol	Output-IF	Application	Application Context
1	↔	TCP	8883	192.168.0.11	vpn0@FW2FW-1-e5XD38H-SMPq		51.144.118.31	SSL	dhcp		CudaloT.azure-devices.net
2	↔	UDP	123	192.168.0.11	vpn0@FW2FW-1-e5XD38H-SMPq		34.200.16.14	NTP	dhcp		
3	↔	UDP	53	192.168.0.11	vpn0@FW2FW-1-e5XD38H-SMPq		8.8.8.8	DNS	dhcp		
4	↔	UDP	123	192.168.0.11	vpn0@FW2FW-1-e5XD38H-SMPq		188.42.216.204	NTP	dhcp		
5	↔	UDP	123	192.168.0.11	vpn0@FW2FW-1-e5XD38H-SMPq		94.228.220.14	NTP	dhcp		

51.137.88.58 Cuda365 51.145.148.47 wmlB

DASHBOARD CONFIGURATION CONTROL FIREWALL VPN LOGS STATISTICS EVENTS SSH

Monitor Live History Threat Scan Audit Log Shaping Users Dynamic Host Rules Forwarding Rules Sync Filter Entries: 17 Max Entries: All Refresh (F5) Disconnect

History Selection Access, Fail, Rule Block, Packet Drop **Traffic Selection** Forward, Local In, Local Out, IPv4, IPv6 **Port** 123

A.	IP Proto	Port	Source	Dest NAT	Interface	User	Destination	Output-IF	Protocol	Next Hop	Application	Application Context	Count	Last	Rule
1	UDP	123	100.64.32.1		vpn0	1-e5XD38H-SMPq	10.16.1.4	dhcp	ntp				31	1s	BLOCKALL



Make it easy

Edit SC

Configuration

Identification Settings

Administrative Settings

WAN Settings

LAN Settings

Wi-Fi Settings

Wireless WAN Settings

VPN Settings

Container Settings


Routing Settings

Firewall Settings

Advanced



Firewall Settings

Firewall Rules



Name	Action	Source Zone
lantovpn	ACCEPT	LAN
lantowifi	ACCEPT	LAN
vontolan	ACCEPT	VPN

Firewall Management

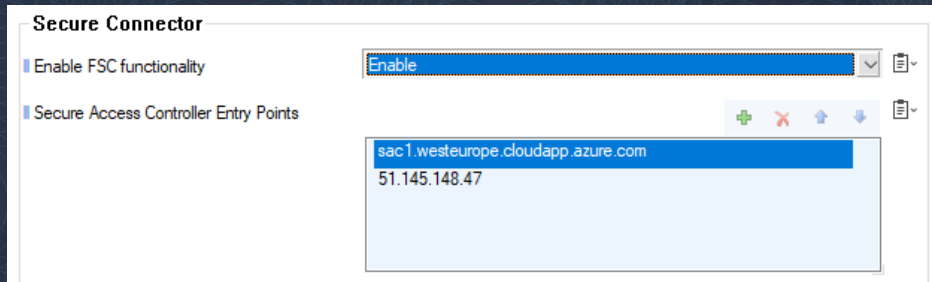


Name	Allow	Source Z...	Services	Descr
lan	1	LAN	SSH , WebUI , ICMP	
vpn	1	VPN	SSH , WebUI , ICMP	
wifi	1	WIFI	SSH , WebUI , ICMP	



Static IP and the cloud

- Use DNS and IP as fallback



- Use static IP in public cloud (not default)

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-ip-addresses-overview-arm#public-ip-addresses>.



Good to know

Default IP is set to 192.168.200.200

Reset: 5 sec for fallback configuration; 10 sec to default

Automatic fallback after 2h since 2.0.7

Add port 22 to your MGMT ruleset – access SSH from Firewall Control Center



Thank you

 Barracuda®
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT