CISCO

You make **possible**

Managing IOx app deployment & connectivity

for IR829/IC3000 using Cisco Field Network Director

Vinay Saini, Solutions Architect @vinsaini
Rishikesh Radhakrishnan, Software Architect @rishikeshr

DEVNET-2560

Barcelona | January 27-31, 2020

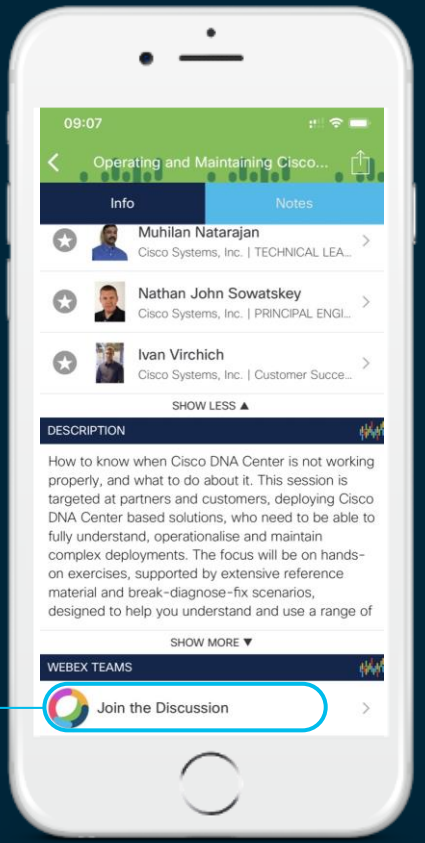
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Agenda

- Introduction
  - Challenges of Deploying & Managing IR829/IC3000 at scale
  - Challenges of Deploying IOx Apps At Scale
  - FND to the rescue
- Managing IR829
  - Local IOx Manager
  - FND Easy mode for Dev Testing
  - Onboarding IR829 to FND
- Managing IC3000
  - Managed vs Standalone modes
  - Setting up Dev Test environment using Standalone mode
  - Onboarding IC3000 to FND
- Tips and Tricks

Your presenters today

- Vinay Saini
- Solutions Architect

- 15+ years in Networking and IoT
- CCIE Wireless#38448, CWNE#69
- Active Contributor to Cisco certification programs.

- Rishikesh Radhakrishnan
- Software Architect

- 15+ years in Software Architecture, Design & Development.
- Focused on IoT, Infra Automation, Multi-Cloud Orchestration.

Introduction

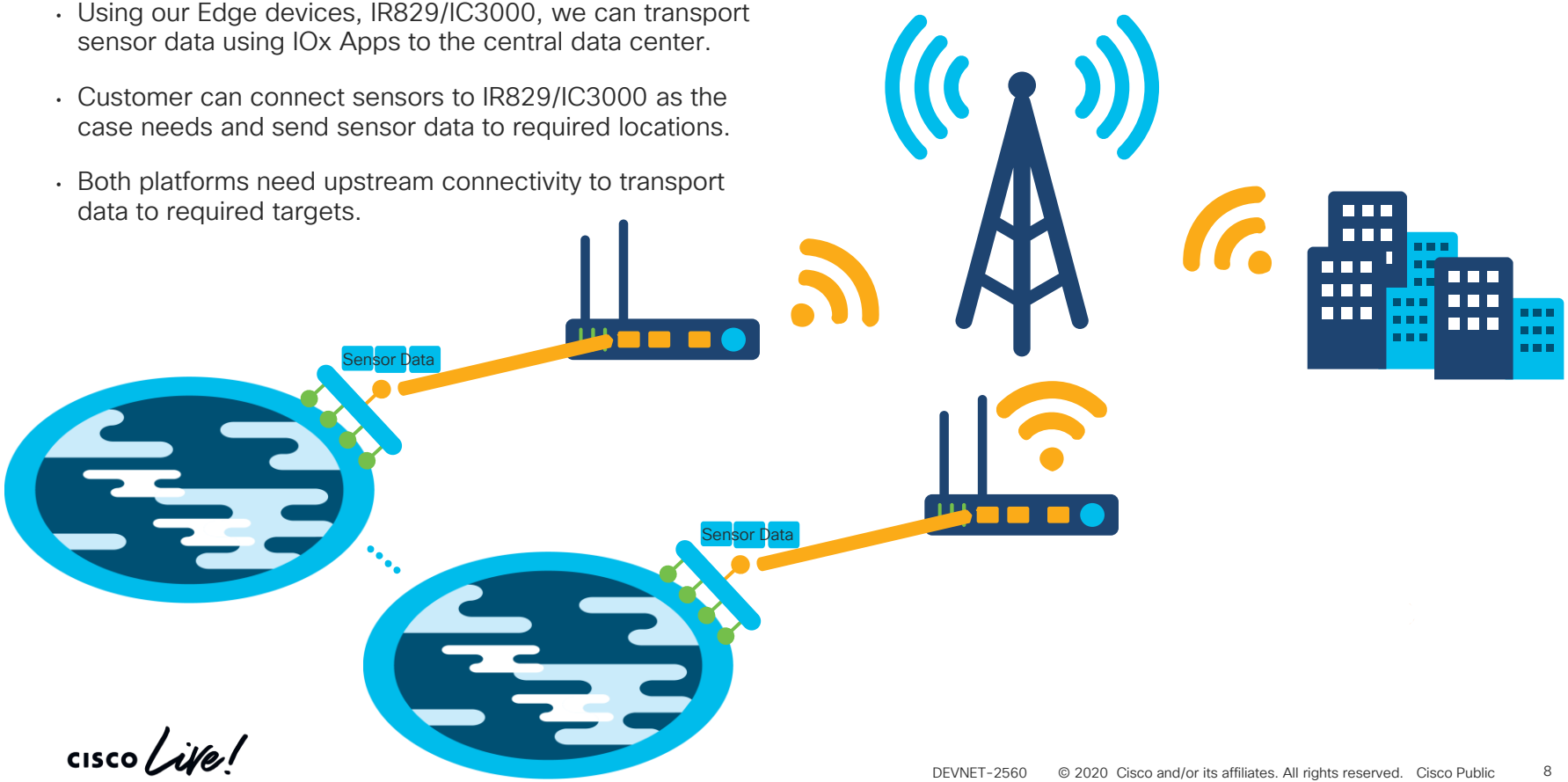
What's going on?

- We have an imaginary nation of Alpha!
- Abundant natural water resources spread across the country.
- Heterogenous terrain across Alpha.
- Uncertain Network availability at remote locations.

- Alpha Goals:
  - Alpha wishes to measure metrics that concern them at their water sources.
  - Water bodies are at various remote locations from the data center.

IoT to the Rescue.

- Using our Edge devices, IR829/IC3000, we can transport sensor data using IOx Apps to the central data center.
- Customer can connect sensors to IR829/IC3000 as the case needs and send sensor data to required locations.
- Both platforms need upstream connectivity to transport data to required targets.



Process

Sensor Setup

Secure Upstream Connectivity

IOx Package Deployment

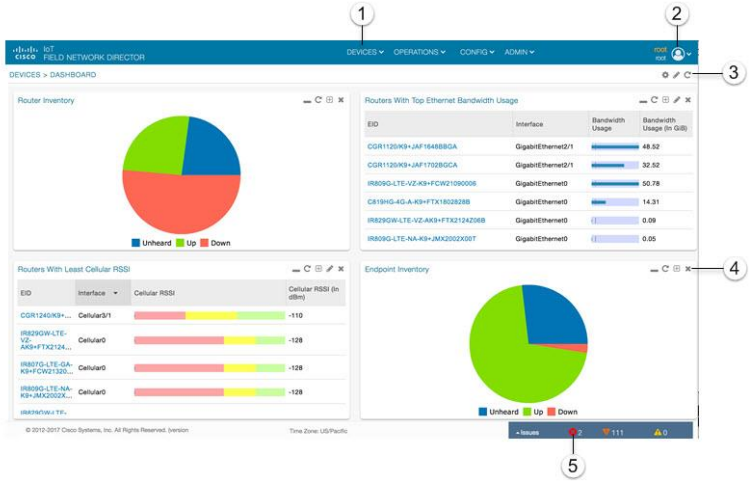
Repeat for 100's of sites

Constraints

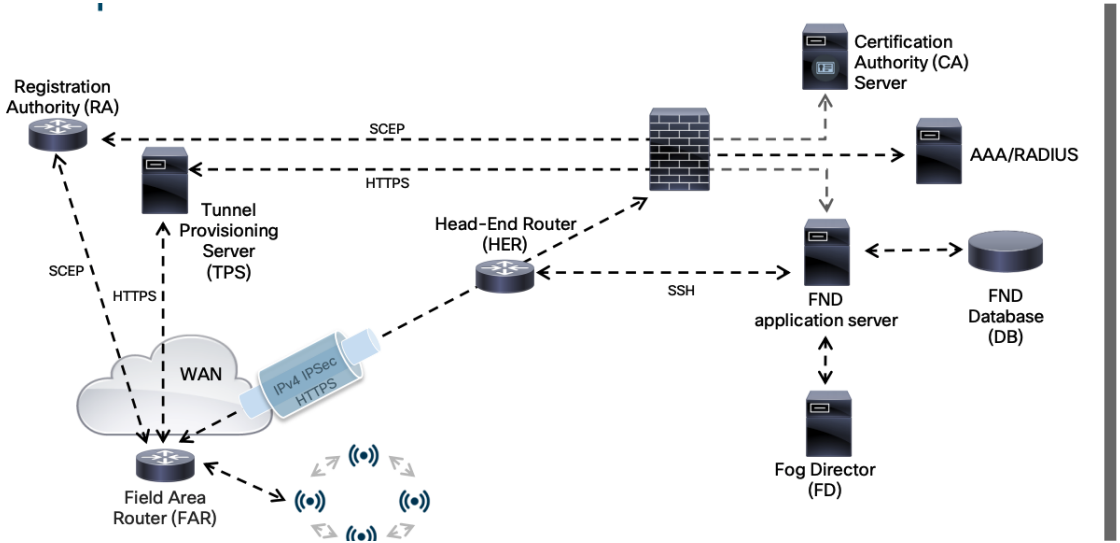
I. *Resource Mobilization.*
II. *Quality.*
III. *Time.*
IV. *Security.*

FND and its connection with FAN

- Allows Zero Touch Deployment
- Remote Application Deployment and management
- Real Time device Monitoring
- Field Device Life Cycle Management



Typical Architecture and Developer Challenges



Fault Isolation is difficult

Firewall

Network Stability Issue

Complex Network between Application and Edge device

Managing IoT Gateways IR8xx

IoT Gateway portfolio

IR807

IR809

IR829

Single & Dual LTE

IR1101

Extending intelligence to operational networks

Ruggedized | Security | High Availability | FOG

Manufacturing	Utility	Transportation/ Public Safety	Oil and Gas	Municipality
• Non-stop operation • Flexible layout change • Deterministic control • Security	• Long-distance connection • Harsh environment • 3G/4G backhaul	• Incident response • Traffic/signal monitoring • Passenger Wi-Fi • Physical security • Video surveillance	• Pipeline monitoring • Long-distance operation • Extreme weather • 3G/4G backhaul	• Intelligent traffic system • Surveillance • City-wide Wi-Fi • Lighting and energy management

IR829
Dual Active LTE+ SSD

mSATA module

Emergency Response Vehicles & Public Safety

Connected Mass Transit & Fleet Management

Ruggedized Remote Applications & Asset Management

Available in U.S, Canada & Europe

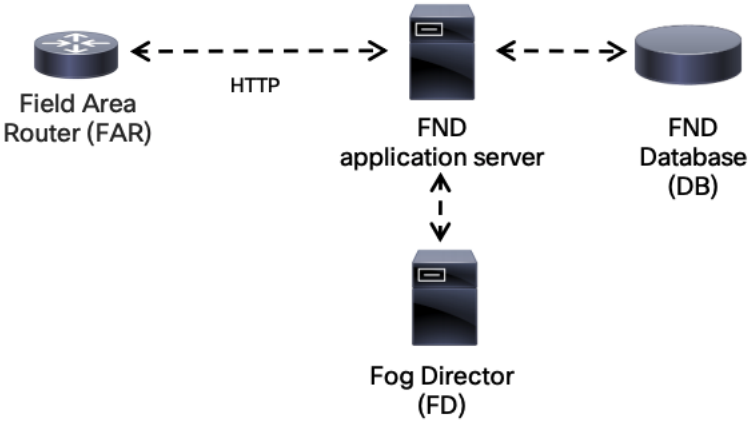
IR829

- **WAN redundancy & high reliability**
- **Higher throughputs** for better user experience
- **Solid & Liquid Protection: IP54**
- **Advanced routing** based on signal strength, cellular technology, etc.
- **Integrated PoE** to power up to four IP devices and **WiFi** connectivity
- **GPS** for location-based services
- **Ignition Power Management** to reduce downtime
- **Accelerometer and Gyroscope** for vehicle/driver safety
- **Fog computing** for intelligence at the edge
- **mSATA storage** option for applications

FND Easy Mode

Easy Mode

- Easy Mode Introduced in FND 4.1
- Minimal working setup without PKI
- No need for a Head End Router (HER) or a tunnel to FND server.
- No need for a Public Key Infrastructure (PKI) setup a Simple Certificate Enrollment Protocol (SCEP).
- No need for router certificates, trustpoint, and SSL certificates.
- All communication is taking place over HTTP instead of HTTPS.



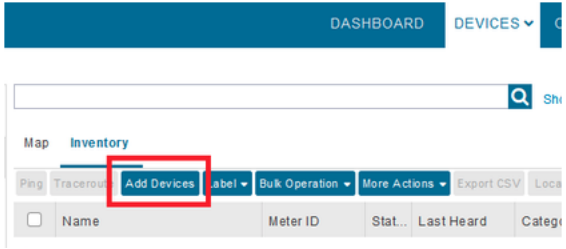
Not for Production use

1 Deploy FND OVF

FND Easy Mode and IR8x9

Configure FND for IR829

1) Edit cgms.properties file
2) Add FND to inventory



3 Add CSV file

2 Enable Easy Mode

```
[root@iot-fnd ~]# cat /opt/fnd/data/cgms.properties
cgms-keystore-password-hidden=dD5KmzJHa64Oyvpqdu8SCg==
use-router-ip-from-db=true
rabbit-broker-ip=
rabbit-broker-port=
rabbit-broker-username=
rabbit-broker-password=
fogd-ip=192.68.5.3
enable-reverse-dns-lookup=false
enableApiAuth=false
fnd-router-mgmt-mode=1
enable-bootstrap-service=true
proxy-bootstrap-ip=10.48.43.231
```

Enables Easy Mode

Enables PNP

Network Settings

Plug and Play Configuration

5A;K4;B2;I10.50.215.252;J9125

5 – DHCP type code 5
A – Active feature operation code
K4 – HTTP transport protocol
B2 – PnP server/TPS/FND server IP address
I10.48.43.231 – FND server IP address
J9125 – Port number 9125

DHCP Option 43

```
ip dhcp pool pnp_pool
network 192.168.10.0 255.255.255.248
default-router 192.168.10.1
dns-server 8.8.8.8
option 43 ascii "5A;K4;B2;I10.48.43.231;J9125"
!
```

For DHCPd on Linux:

```
[jedepuyd@KJK-SRVIOT-10 ~]$ cat /etc/dhcp/dhcpd.conf
subnet 192.168.100.0 netmask 255.255.255.0 {

option routers 192.168.100.1;
range 192.168.100.100 192.168.100.199;
option domain-name-servers 192.168.100.1;
option domain-name "test.dom";
option vendor-encapsulated-options "5A;K4;B2;I10.48.43.231;J9125";
}
```

Static PnP

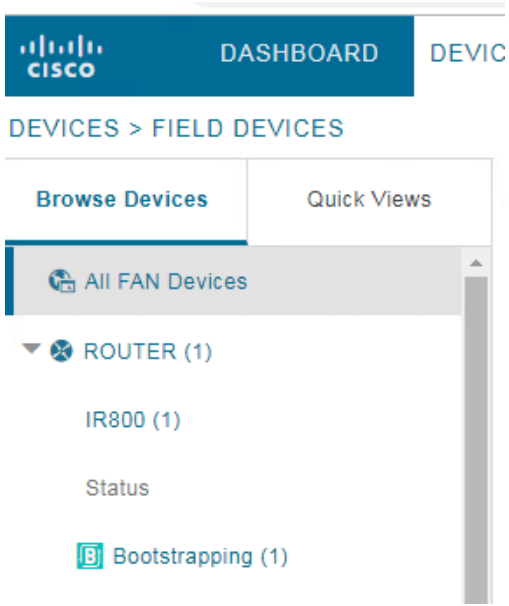
4 Point IR to FND

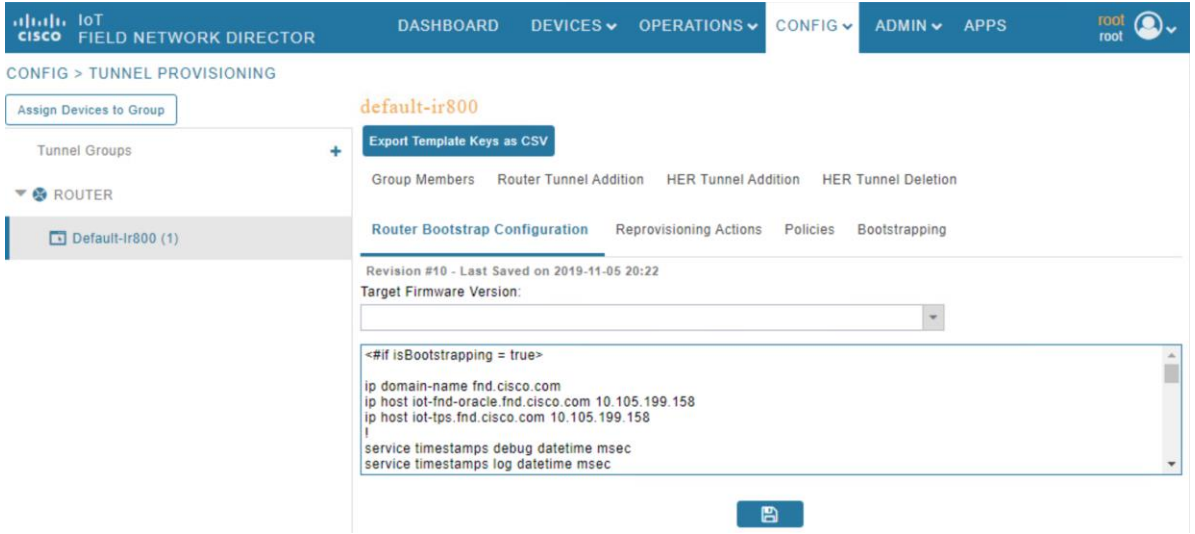
```
IR800(config)#pnp profile pnp-zero-touch
IR800(config-pnp-init)#transport http ipv4 10.48.43.231 port 9125
IR800(config-pnp-init)#end
```

FND – Bootstrapping IR829

5

Configure > Tunnel Provisioning > Router Bootstrap Configuration





Troubleshoot

From FND

FND Logs – **/opt/fnd/logs/server.log**

FND GUI: **Devices > Inventory > Select Device > Events**

From IR829

show cgna profile-state all
debug cgna logging

Most Bootstrapping issues happens due to syntax errors in template.

Managing IC3000

IC3000: IoT Edge Compute gateway

Cisco Software Security

- Trusted Cisco Linux kernel with regular security updates (PSIRT)
- Secure boot, signed apps, secure connectivity

Cisco Hardware Security

- Hardware based anti-counterfeit, anti-tamper chip
- Hardware root of trust for secure boot and data

Management of compute appliances

- Device, Network, and app life-cycle management at scale with Field Network Director
- IOx Edge compute framework for application container management

Hardware Specs

- 4 Core Intel Rangeley 1.2 GHz (I-temp)
- 8-GB DRAM (soldered down)
- mSATA SSD 128 GB
- Compact DIN rail unit design
- 2 Gigabit Ethernet Copper ports and 2 SFP Fiber ports

New in IC3000 with version 1.2.1

New Standalone Mode

- Developer mode replaces with Standalone mode.
- Removes hassle of creating separate credentials via Console
- Direct access to IOx Manager with default Credentials

Developer Mode → Standalone Mode

Production Mode → Managed Mode

IC3000 as Cyber Vision Sensor

Standalone Mode

- Standalone mode operates by default over a predetermined IPv4 Link-local addresses (169.254.128.x). First Step before Remote Management is enabled
- Standalone mode CANNOT be turned ON via FND.

Management Interface Configuration	Laptop Configuration
IP address 169.254.128.2	IP address 169.254.128.4
Netmask 255.255.0.0	Netmask 255.255.0.0

Standalone Mode – Remote Access

Allows IOx manager access over LAN

Access over routable configured IP

Cisco Systems
Cisco IOx Local Manager

Hello, test2 | Log Out | About

Applications | Cartridges/Layers | System Info | System Setting | System Troubleshoot | Device Config

Data Interface Config

Interface	IP Address	Action
svcbr_0	33.33.33.33	edit | view
int1	22.22.22.22	disable | edit | view
int2	...	disable | edit | view
int3	...	enable | edit | view
int4	...	enable | edit | view

Software Upgrade

Select Image: Choose File No file chosen

Upload & Install

Refresh

User Config

Name: test2

Change Password

Developer Mode

Developer Mode: On

Developer Mode Off

Remote Device Management: Enabled

Disable Remote Management

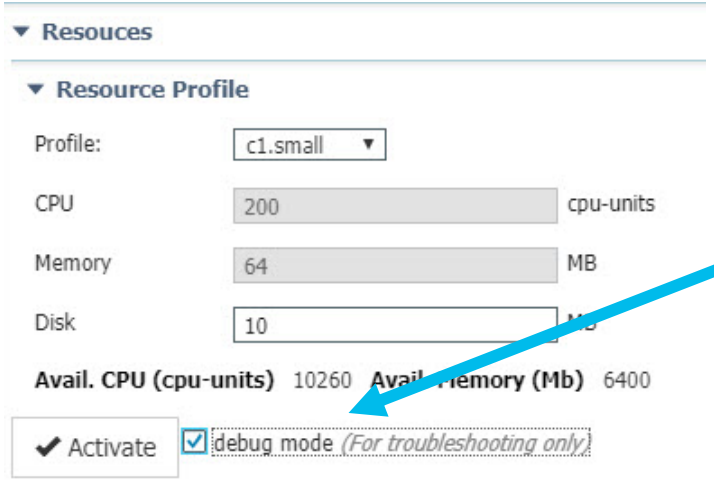
Default Route

Gateway IP: Interface:

Set Default Route

Troubleshooting IC3000

App Troubleshoot – Debug Mode



Prevents the application container from stopping when your application terminates unexpectedly.

App Troubleshoot – Console Access

1. Create & save PEM certificate.
2. Get the private key of the container
3. Save the private key by copying the entire content into the *<pemFileName>* **.pem** file you created in step 2
4. Add the necessary permissions for the file. Recommended using "chmod 600”
5. SSH to application console

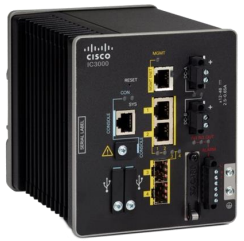
ssh -p {SSH_PORT} -i <pemFileName>.pem appconsole@169.254.128.2 {SSH_PORT} = 22

IC3000 Managed Mode

IC3000 and FND

IC3000 supports only HTTPS

FND Easy mode will not work



IC3000

HTTPS only

LAN

FND Application Server

- OVF deployment is same – No need to edit cgms.properties
- IR829 will also join in this mode. (Requires relevant certificates)

Managed Mode

Device configuration and application lifecycle management via Cisco Field Network Director (FND).

1. Option 43 settings in DHCP

No Manual config

2. Adding IC3000 to FND using CSV

3. Config Template

FND 4.3 : GUI based
From FND4.3.1: JSON Format

https://www.cisco.com/c/dam/en/us/td/docs/routers/ic3000/deployment/guide/IC3000-JSON.txt

IC3000 Config Template

IoT FIELD NETWORK DIRECTOR

DASHBOARD | DEVICES | OPERATIONS | CONFIG | ADMIN | APPS

root root

CONFIG > DEVICE CONFIGURATION

Assign Devices to Group | Change Device Properties | default-ic3000

Groups

Configuration Groups +

- ROUTER
  - Default-Ir800 (1)
- GATEWAY
  - Default-Ic3000 (1)

Group Members | Edit Configuration Template | Push Configuration | Group Properties

Current Configuration revision #2 - Last Saved on 2019-11-05 21:55

Select Configurations

- [x] Periodic Metrics Management Profile
- [x] Heart Beat Management Profile
- [x] IOx Credentials
- [ ] User Credentials
- [x] IPv4 Interface Settings
- [ ] IPv6 Interface Settings
- [ ] IP Static Route Settings
- [ ] DNS Configuration
- [ ] NTP Server Configuration

Periodic Metrics Management Profile

Interval: 300

Heart Beat Management Profile

Interval: 60

IOx Credentials

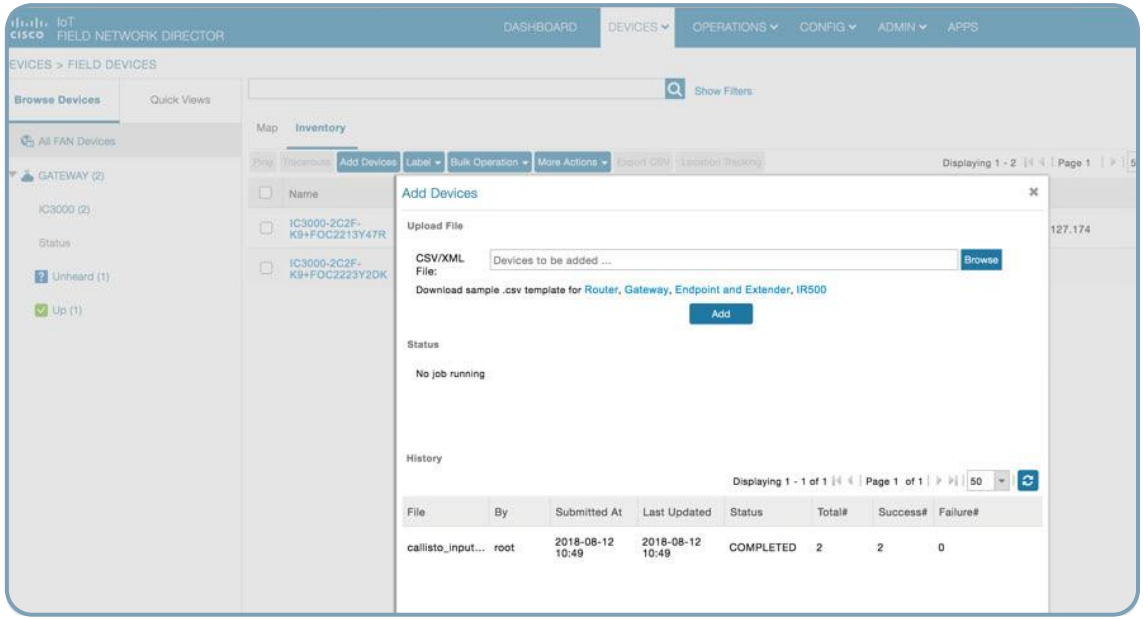
IOx Username: Use property 'IOxUserName'

IOx Password: Use property 'IOxUserPassword'

IPv4 Interface Settings

Managed Mode

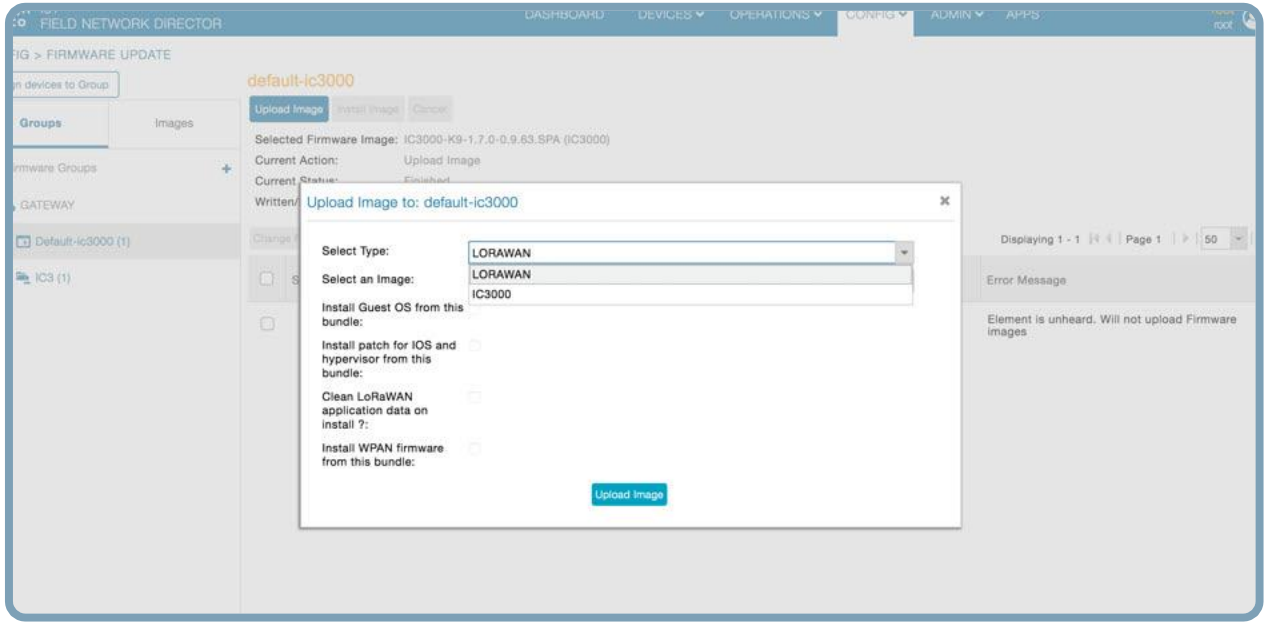
- Click DEVICES>FIELD DEVICES>Inventory>**Add Devices**. Browse to the location of your excel spreadsheet and click Add.



Managed Mode

- Upgrading Firmware with FND

Select **CONFIG>Firmware update>Select the device group>Upload Image**
Once the Image upload is complete, select the Install Image tab and proceed with upgrading the firmware.



Application Deployment

IoT FIELD NETWORK DIRECTOR

DASHBOARD | DEVICES | OPERATIONS | CONFIG | ADMIN | APPS

root root

APP MANAGEMENT

Import New App

IOx Package | OVA | Docker

Upload an application package created via the IOx SDK.

Package File: Select ...

Import

Tips & Tricks

IC3000 Troubleshooting

Standalone Mode

To debug Application status use the **APP Tab**

- APP logs :**APP Tab > Manage APP > APP-Dir** or **App-Logs** and download the logs.
- Application failure : **System Troubleshooting Tab** :Provides events or errors.

IC3000 Provisioning via FND

- Check the option 43 address format, and validate if it is the correct ip address of FND
- **show ida** status and **show interfaces** status to see which ip address the device has learned.
- Check the FND provisional setting URL to ensure FND IP address:9121
- Check whether the serial number in the FND input file is accurate

Failed Upgrade via FND

IoT FIELD NETWORK DIRECTOR — DASHBOARD | DEVICES | OPERATIONS | CONFIG | ADMIN | APPS — root root

CONFIG > FIRMWARE UPDATE

Assign devices to Group

Groups | Images

Firmware Groups +

- ROUTER
  - Default-Ir800 (1)
- GATEWAY
  - Default-Ic3000 (1)

default-ic3000

Upload Image | Install Image | Cancel

Selected Firmware Image: IC3000-K9-1.1.1.SPA (IC3000)
Current Action: Upload Image
Current Status: Finished
Written/Devices: 0/1
Error/Devices: 1/1

Change Firmware Group

Displaying 1 - 1 | Page 1 | 50

Address	Firmware Version	Activity	Update Progre...	Last Firmware Status Heard	Error Message	Error Details
:.168.89.55	1.0.1	ERROR	100%	2019-12-10 21:47:28	Unable to upload Firmware image: java.lang.Exception: Device failed to get image from FND	Click to View

Check Provisioning URL

IoT FIELD NETWORK DIRECTOR — DASHBOARD | DEVICES | OPERATIONS | CO

ADMIN > SYSTEM MANAGEMENT > PROVISIONING SETTINGS

Provisioning Process

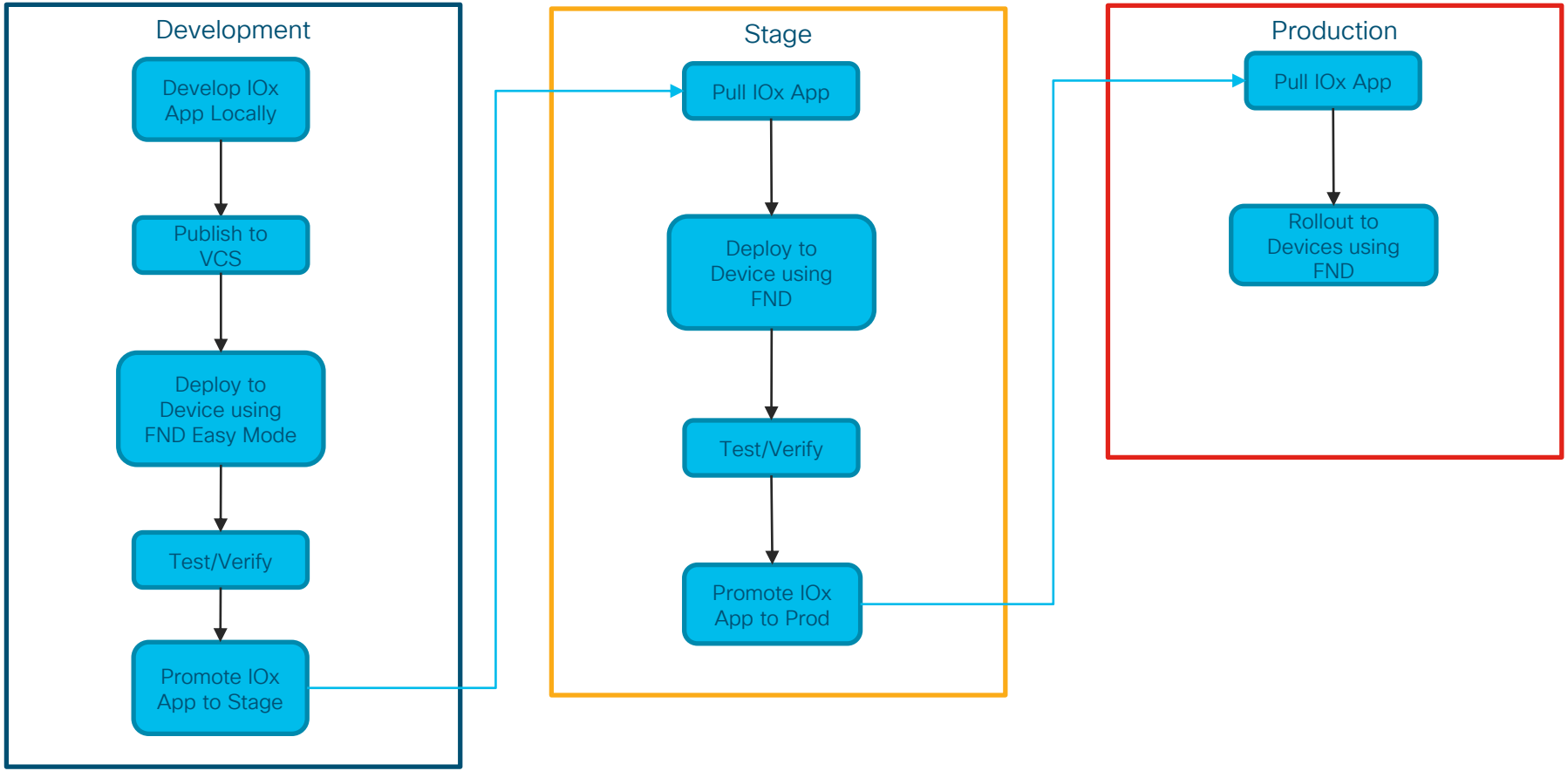
IoT-FND URL: https://192.168.89.10:9121

Field Area Router uses this URL to register with IoT-FND after the tunnel is configured

Periodic Metrics URL: https://192.168.89.10:9121

Field Area Router uses this URL for reporting periodic metrics with IoT-FND

Development/Deployment Flow



Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**