RTX
WIRELESS WISDOM

RTX3300 WMTS
Smart-Hopping 2.0
USB Access Point

Version 1.0

© September-2021 RTX A/S, Denmark

Trademarks

RTX and the combinations of its logo thereof are trademarks of RTX A/S, Denmark.

Other product names used in this publication are for identification purposes and maybe the trademarks of their respective companies.

Disclaimer

The contents of this document are provided about RTX products. RTX makes no representations with respect to completeness or accuracy of the contents of this publication and reserves the right to make changes to product descriptions, usage, etc., at any time without notice. No license, whether express, implied, to any intellectual property rights are granted by this publication

Confidentiality

This document should be regarded as confidential, unauthorized copying is not allowed

© September-2022 RTX A/S, Denmark, All rights reserved

http://www.rtx.dk

Table of Contents

About This Guide

Audience

Who should read this guide? This guide is intended for qualified service personnel who will install, configure, and service the IntelliVue Smart-hopping 2.0 Access Point as a part of an overall IntelliVue Clinical network.

When should I read this guide?

Read this guide before you install the USB Access Point to your existing Cisco Network.

This manual will enable you to set up components in your network to communicate with each other and deploy a fully functional IntelliVue Smart-Hopping Patient Monitoring System.

Important Assumptions

This document was written with the following assumptions in mind:

1)You understand network deployment in general

2)You have working knowledge of basic TCP/IP/SIP protocols, Network Address Translation, etc...

3)A proper site survey has been performed, and the administrator have access to these plans

Document organization

WHERE IS IT?	CONTENT	PURPOSE
CHAPTER 1	Introduction to the Philips IntelliVue Smart-Hopping 2.0 Patient Monitoring	To gain knowledge about the different elements in a Philips IntelliVue Smart-Hopping 2.0 Network and the purpose of the USB AP
CHAPTER 2	SH 2.0 Deployment	Guides you through the process of deployment of your SH 2.0 USB AP System
CHAPTER 3	Installation and Configuration	Mounting and installation procedures step by step.
CHAPTER 4	Interaction with the PiC iX	Table with all the new alarms that can be seen in PIC iX UI.
CHAPTER 5	Troubleshooting	Alarms related to OTAS and basic troubleshooting procedures.
CHAPTER 6	System Update	Things to consider before updating the different parts of your system. Guides you through the update process.
APPENDIX B: FIRMWARE UPDATE		
APPENDIX C:		

Document History

REVISION	AUTHOR	ISSUE DATE	COMMENTS
First draft	LIP	xx-Feb-2023	

What is new

What new features have been added.

VERSION	FEATURE
V1	New document

Related Documentation

Philips IntelliVue Smart-hopping 2.0 Access Point Controller Installation Guide - provides procedures for physically installing and powering the Smart-hopping Access Point Controller at the clinical site.

Smart-hopping 2.0 Infrastructure Installation and Service Guide - provides complete information and procedures to install, configure, inter-connect, and deploy the Smart-hopping infrastructure at the clinical site. This document includes site planning guidelines, procedures for use of the APC command line and graphical user interfaces, Access Point configuration procedures, and APC and Access Point firmware deployment procedures.

Smart-hopping Synchronization Unit Installation Guide – lists procedures to install the Smart-hopping Sync Unit at the clinical site.

Smart-hopping 2.0 Upgrade Guide - gives instructions on upgrading Philips Smart-hopping infrastructure (Access Points and Access Point Controllers)

Abbreviations:

Table of abbreviations:

ABBREVIATION	MEANING
AP	Access Point
APC	Access Point Controller
BTLE	Bluetooth Low Energy
DNAC	Cisco DNA Center
LAN	Local Area Network
OTAS	Over-the-air Synchronization
PIC iX	Patient Information Center iX
SH USB AP	Smart- Hopping USB Access Point
VAP	Virtual Access Point
WMTS	Wireless Medical Telemetry Service
WLC	Wireless LAN Controller

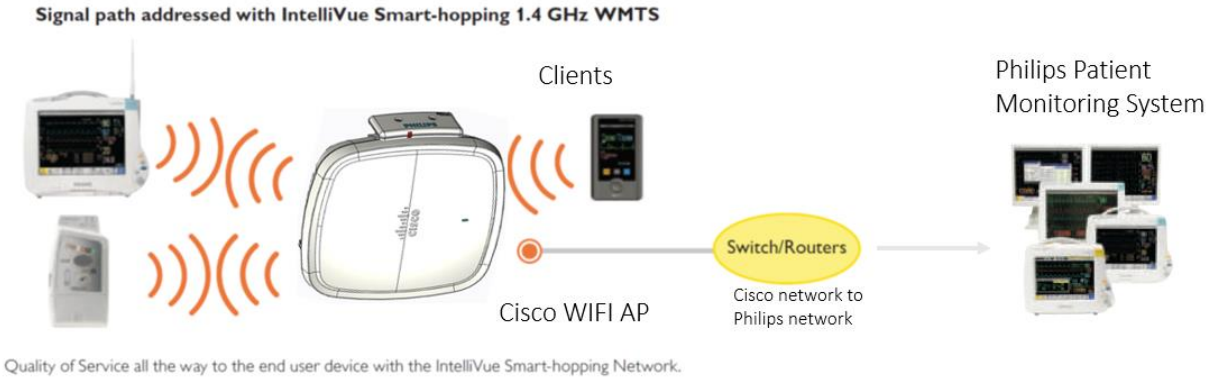
Chapter 1: Overview

Introduction

//Introduction of the IntelliVue Smart-Hopping and what purpose does the USB AP serve in it.

The RTX3300 Smart-hopping USB Access Point is designed as a part of the Philips IntelliVue Smart-hopping 1.4 GHz WMTS and aids in the communication of wireless client WMTS devices (patient sensors, that perform patient monitoring services) with the rest of the Philips Patient Monitoring System via the Cisco Wi-Fi Access Point (see Figure.1. below). The USB AP should be installed on the already existing Smart-hopping 2.0 infrastructure with PIC iX (Patient Information Center iX) and Access Point Controller, installed according to the applicable Philips Documentation (see *Smart-hopping 2.0 Infrastructure Installation and Service Guide*).

Figure.1. The RTX3300 Smart-hopping USB Access Point in the IntelliVue Smart-hopping network.


Signal path addressed with IntelliVue Smart-hopping 1.4 GHz WMTS
Clients
Philips Patient Monitoring System
Switch/Routers
Cisco WIFI AP
Cisco network to Philips network
Quality of Service all the way to the end user device with the IntelliVue Smart-hopping Network.

The purpose of the RTX3300 USB device is to enable a patient monitoring access point (AP) using the already existing enterprise grade Wi-Fi infrastructure platform, instead of having a special wired network with sync capability. It is designed to work with the Cisco Catalyst 9120/30 Wi-Fi Access Points and there is no need to install new cables or make any other costly modifications to the whole site.

The WMTS USB AP is fully compatible with the RTX3481 Smart Hopping 2.0 Access Point and there will be no difference seen from the WMTS Client devices' side. One system can contain both Smart-Hopping 1 and Smart-Hopping 2.0 APs and RTX3300 APs, and client devices can roam seamlessly between them.

If multiple USB AP are used, they can be organized in zones and synced in sync trees that allows seamless roaming of the patients in the hospital. Using Over-the-air Synchronization (OTAS) makes it easier to sync without the need for a sync box.

Cisco (and other brands) provides a range of metal and plastic enclosures for their Wi-Fi APs. Some of those enclosures aren't fitting after mounting the USB AP, and others, like the metal ones, are going to interfere with the RF signal and are not recommended. The *Oberon 1018-00 Wi-Fi Access Point non-metallic, low-profile, recessed, or in-wall mount enclosure* is one of the recommended ones.

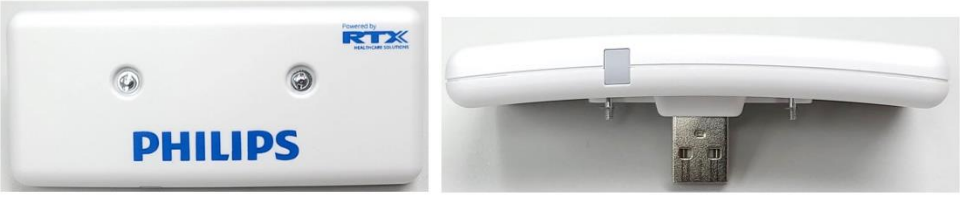
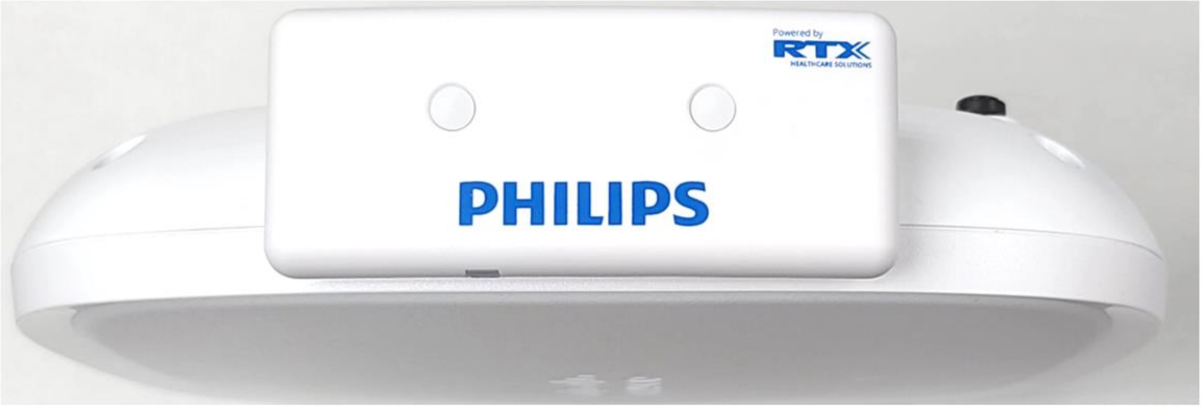
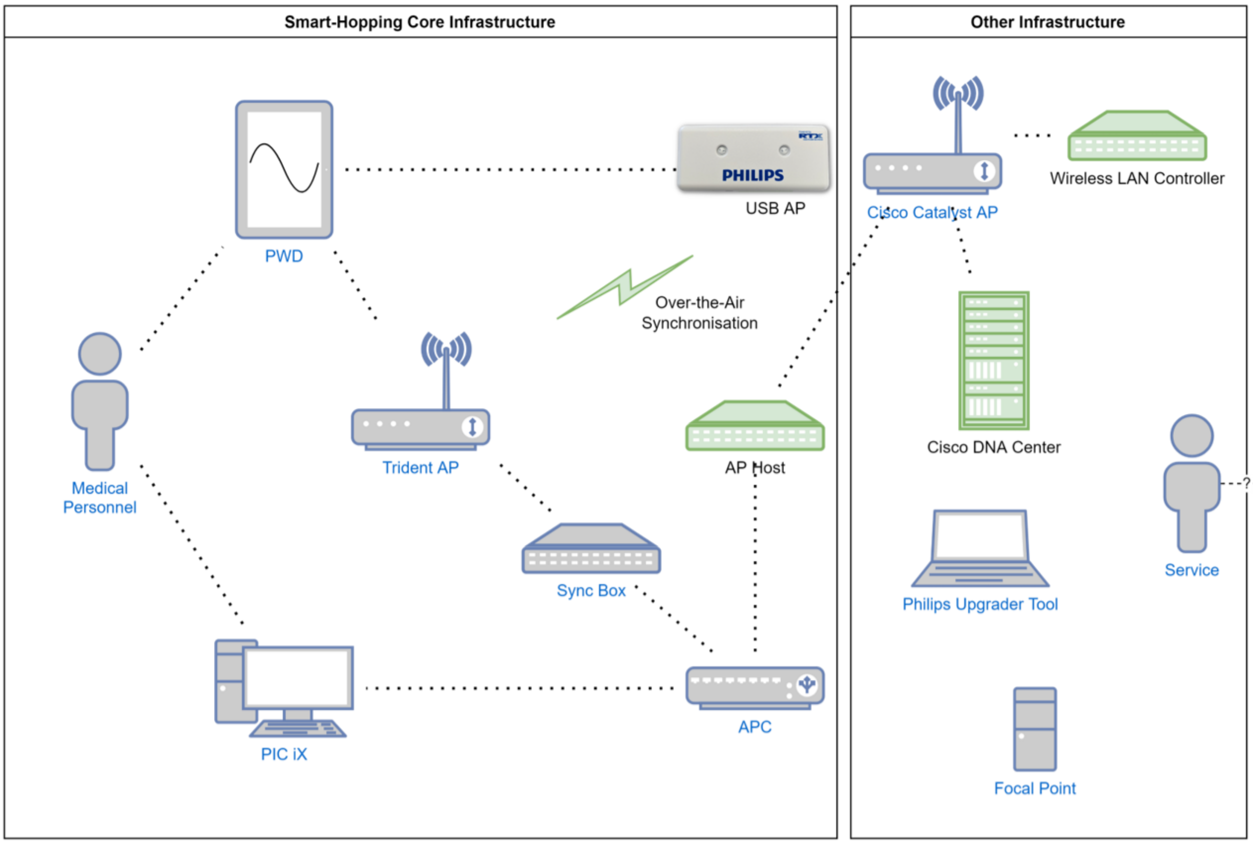


Figure.2. RTX3300 Smart-Hopping USB Access Point.



Network Components



The IntelliVue Smart-hopping Network consists of an Ethernet LAN that can include LAN switches and routers and is used to interconnect multiple IntelliVue Access Points to one or more Philips Access Point Controllers (APC).

The key function of the IntelliVue Smart-hopping Network is to transport data from the IntelliVue Client WMTS devices (sensors, heart monitors, pulse monitors, etc.) over a wireless LAN-based infrastructure (part of the IntelliVue Clinical Network) to/from the IntelliVue Information Center where the data can be recorded or used to alert clinical operators(personnel) as to a change in monitored parameters.

Major components comprise the Philips IntelliVue Smart-hopping Infrastructure:

- Smart-hopping USB Access Point
- Cisco Catalyst Wi-Fi Access Point
- Cisco Patient Information Center Interface - PiC iX
- Access Point Controller
- AP Host
- Cisco DNA center
- Synchronization Box
- Wireless LAN Controller?
- Uninterruptible Power Supply

The **Smart Hopping USB Access Point** connects to the **Cisco Catalyst** 9120/30 WiFi Access Point and together these two units serve as a WMTS Access Point and have the same functionality as the Smart Hopping 2.0 Access Point (Dedicated Intern AP) – providing the interface between the client WMTS devices and the wired network. However, compared to it they have the following advantages:

- Easy integration, installation, and maintenance as part of the already existing network.
- Can be used with the existing Cisco infrastructure.

The 2 units are able to work together with the help of the **IOx application**, that needs to be installed in advance on the Wi-Fi AP via the DNA center. Once installed the IOx application helps connect the SH USB AP to communicate with the rest of the Smart- Hopping infrastructure.

The application hosting on the Cisco AP is enabled by the **Cisco DNA Center** (DNAC). That is a network controller and management platform. It helps us install the IOx application to the Cisco Wi-Fi AP. That is essential for the Wi-Fi AP to be able to recognize the USB AP as a part of the SH network.

The **Access Point Controller (APC)** is a Philips unit that administers, controls, and configures the SH APs in the system. From the APC side the SH USB AP is seen in the same way as the Smart- Hopping 2.0 AP. (Radio wise, bandwidth wise, and telemetry-data-protocol wise the RTX3300 based Access Points are 100% compatible with the RTX3481 Smart Hopping 2.0 Access Point. So, seen from the Client WMTS devices there are no differences.)

The AP Host is a Linux based unit, that virtualizes the access points and communicates with IOx application. It works as a bridge between the new system and the old IntelliVue system. The AP Host creates virtual APs and aids the communication between the SH USB AP, the Cisco Catalyst Wi-Fi AP, and the APC. This unit also handles the OTAS synchronization of the USB AP devices in the system. The wired time-synchronization for dedicated Smart-Hopping Access Points is provided by the **Synchronization Box.**

The data received from the wireless client WMTS devices is represented in a user-friendly way via the **Patient Information Center iX (PIC iX).**

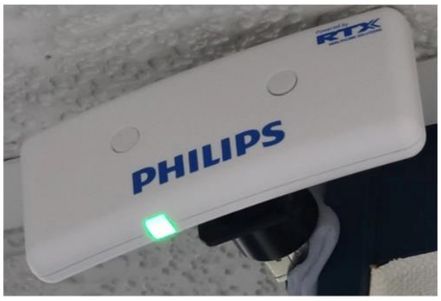
The **Wireless LAN Controller (WLC)** is part of the Cisco network, that manages the Cisco Catalyst Wi-Fi Access Point.

Sync Box is part of the Philips network in charge of synchronizing the different trident aps. In the RTX3300 the Sync box is replaced by **OTAS Controller** that provides service and configuration needed for the SH USB AP to maintain Radio Frame synchronization.

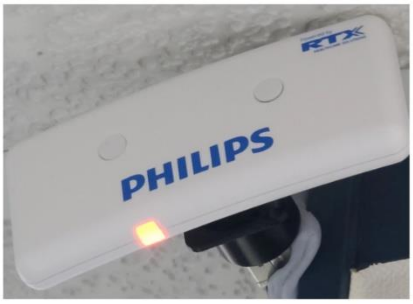
LED Status Indicators

The Smart-Hopping USB AP unit is equipped with a 3 color LED indicator that flickers to indicate correct startup operation. One of the LEDs (LED3 on the table below) indicates the presence of radio signal and the other two change color depending on the status of the Access Point. Table.1. summarizes the status of the USB Access Point LEDs. On the pictures below can be seen the different colors of the LED indicator.

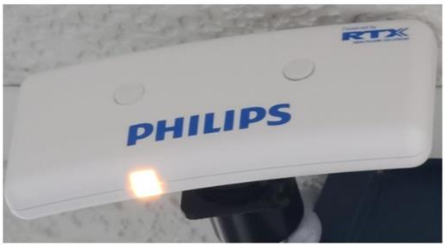
Green color



Red color



Yellow color



Blue color

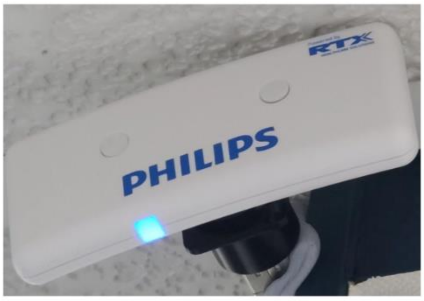


Table.1. USB AP Status LED patterns.

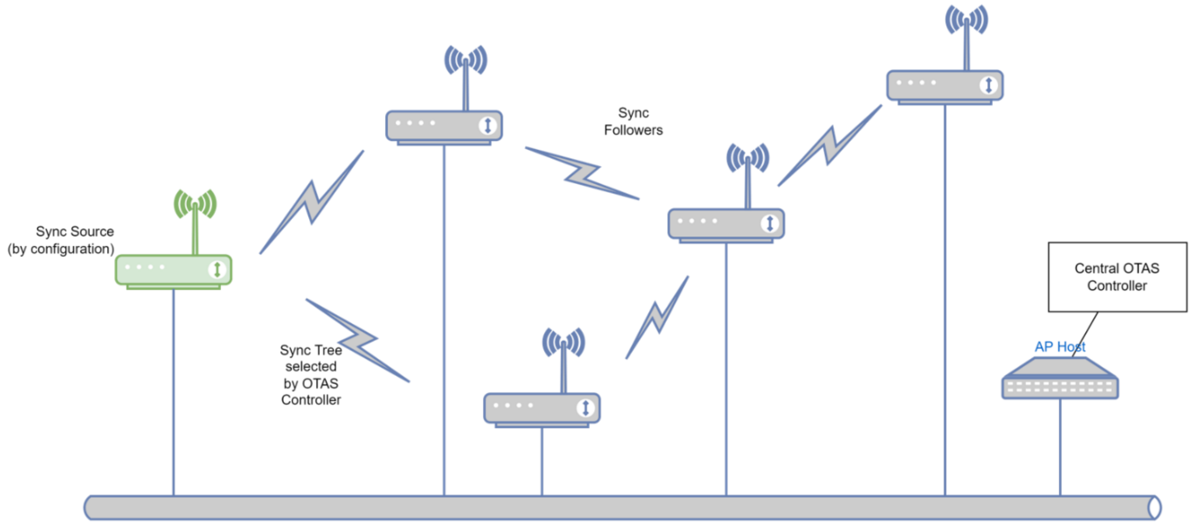
LED1(500ms)	LED2(500ms)	LED3(100ms)	Status
● **No light**	● NO light		Access Point either does not have power or configured to turn the LEDs off.
🔴 **Solid red**	🔴 Solid red		Power On, if seen for more than 5 seconds, replace unit
🟠 **Solid amber**	🟠 Solid amber		Booting & connecting, not yet connected to APC
🔴 **Flashing red**	● NO light		Hardware failure, POST failure
🟠	●		Connected to AP Host, Establishing sync

Flashing amber	NO light		
● **Dim green**	● Dim green	● Bright green	Connected to APC, Radio Signal is Active
● **Flashing green**	● Flashing red		Lost sync source
● **Solid blue**	● Solid blue		FL7 mode
● **Blinking blue**	● NO light		Firmware download mode

Supported Topologies and System Limits

Topologies

Over-the-air Synchronization (OTAS) is a wireless alternative of Philips SH 1.0 and SH 2.0 wired synchronization. In SH 2.0, the system relies on the Sync Box to serve as a timing source and ensure all APs in the system are synchronized. That is required for the portable devices to roam around and do handover between the APs. The sync tree ordered structure of APs is letting all the APs in the tree to follow the same timing as the primary AP.



In RTX3300 the system relies on the OTAS controller, located in the AP Host, to handle the synchronization process. Installing personnel needs to define primary and secondary sync source and the OTAS controller will decide the sync tree.

The Philips SH 2.0 system uses a centralized server to collect the OTAS information and signals the RTX3300 how to synchronize to the self-formed OTAS tree.

When deciding OTAS sync trees it is essential that the paths to the sync source are as short as possible and to ensure redundancy it is crucial that there is more than one paths possible to the sync source.

Chain structures are not recommended for redundancy reasons. They are least reliable in case of one of the AP falling out of the system (losing power, network, etc.). Therefore, the best way to organize your zones is in a sync tree. Examples can be seen in the figures below.

Fig.XX. OTAS Sync Trees:

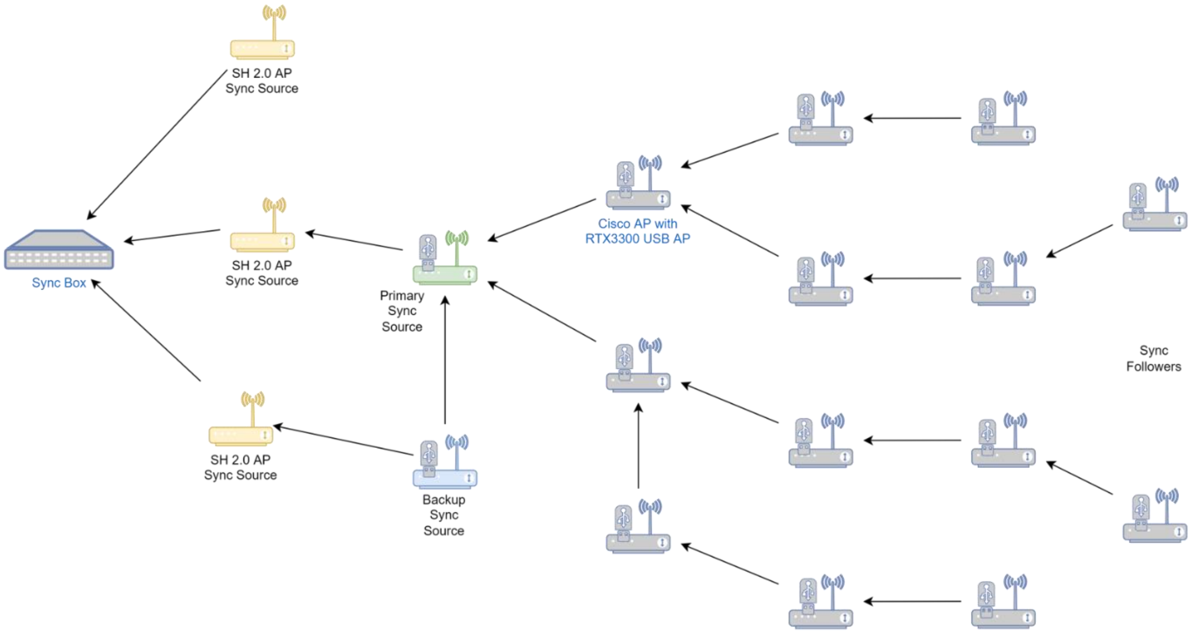


Fig.xx. Multiple zones with external SH 2.0 AP sync:

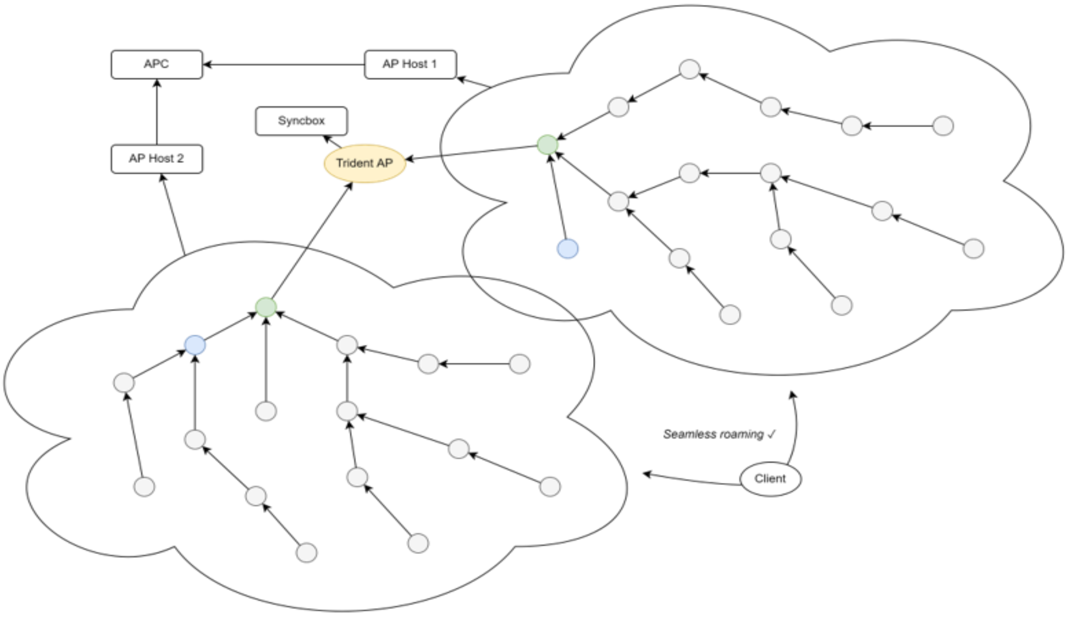
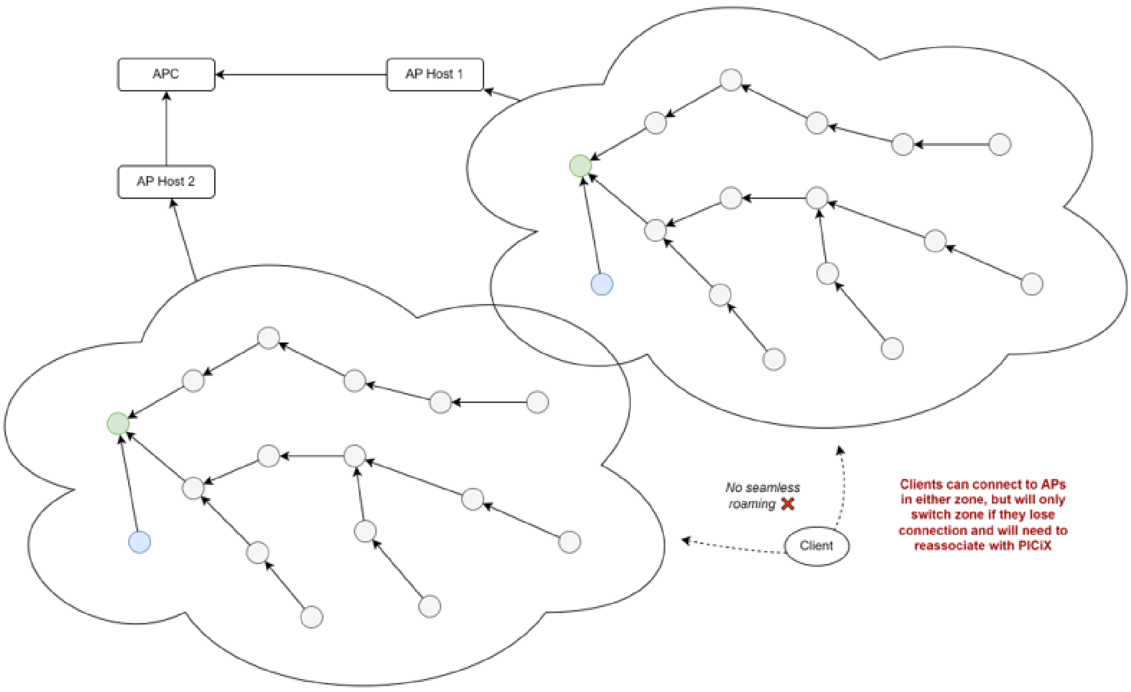


Fig.xx. Multiple zones without external sync:


APC
AP Host 1
AP Host 2
No seamless roaming
Client
Clients can connect to APs in either zone, but will only switch zone if they lose connection and will need to reassociate with PICiX

OTAS Limitations

These are the limitations set by Over-the-air Synchronization (OTAS) that the user has to be aware of:

- OTAS supports **maximum of 16 USB APs per zone**.
- **Primary and secondary sync source are static**. They have to be predefined upon generating the sync tree. The MAC addresses of chosen primary and secondary units are recorded in the OTAS controller.
- In cases when more than one sync trees are required in the hospital, **external sync is necessary**. That external sync unit is predefined and has to be an SH 2.0 AP.
- In case of multiple sync trees in the hospital it is recommended that overlapping between the zones is not significant.
- For better performance all systems withing RF range should share sync.

Infrastructure specifications

Host devices

Only to be used with approved devices from the RTX host devices list.

Safety Regulatory Compliance

FCC Compliance:

Operation of this equipment requires the prior coordination with a frequency coordinator designated by the FCC for the Wireless Medical Telemetry Service. The transceiver and the Smart-hopping infrastructure are subject to radio frequency interference. If suspected radio frequency interference with your device, contact your service provider. This device complies with Parts 15, 27 and 95H of the Federal Communications Commission (FCC) Rules. Operation is subject to the condition that this device does not cause harmful interference.

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and any part of your body.

FCC-ID To be determined

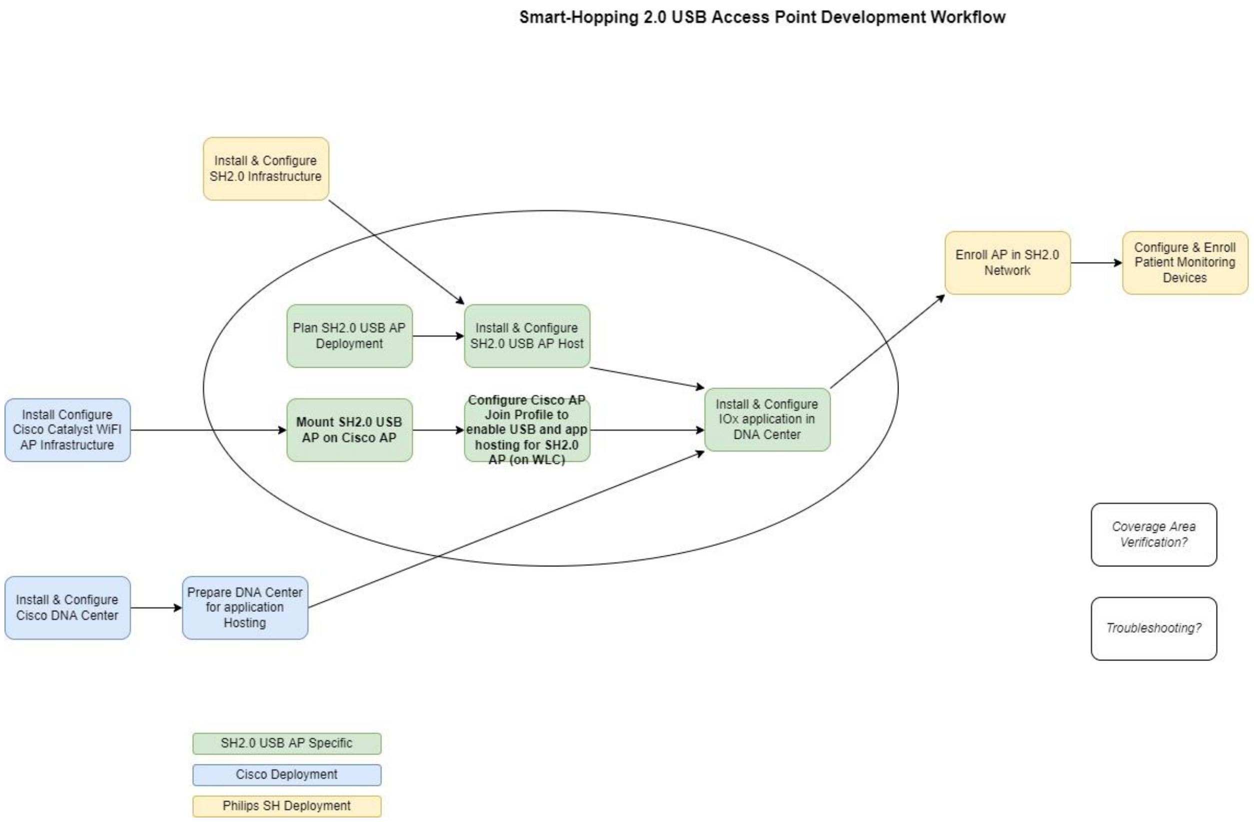
Environmental Specifications?

What temperatures and humidity can it work in. Environmental test results.?

Chapter 2: SH 2.0 Deployment

The USB is designed to aid setting up the IntelliVue smart hopping patient monitoring system on an already existing Cisco network. This chapter presents the things to consider before installing your USB AP and setting up the system.

The chart below visualizes the SN 2.0 USB AP development workflow and the responsible sides.


Smart-Hopping 2.0 USB Access Point Development Workflow
Install & Configure SH2.0 Infrastructure
Plan SH2.0 USB AP Deployment
Install & Configure SH2.0 USB AP Host
Install Configure Cisco Catalyst WiFI AP Infrastructure
Mount SH2.0 USB AP on Cisco AP
Configure Cisco AP Join Profile to enable USB and app hosting for SH2.0 AP (on WLC)
Install & Configure IOx application in DNA Center
Enroll AP in SH2.0 Network
Configure & Enroll Patient Monitoring Devices
Coverage Area Verification?
Troubleshooting?
Install & Configure Cisco DNA Center
Prepare DNA Center for application Hosting
SH2.0 USB AP Specific
Cisco Deployment
Philips SH Deployment

System Requirements

Here is what your system needs to have already available, before starting with your deployment process:

- ✓ Existing Cisco network with all the required infrastructure: WLC, DNA center, Cisco Catalyst 9120/9130/9136 APs. All Cisco Wi-Fi Access Points are already placed and installed and running a working WLAN network.
- ✓ Installed and Configured Cisco DNA Center, ready for application hosting.
- ✓ Installed and configured SH 2.0 Infrastructure: clients, sync box, PIC iX
- ✓ Make sure your software versions are matching
- ✓ Make sure the USB port on Cisco Access Points in enabled. Requirements for that might affect power supply recommendations.
- ✓ RSSI recommendation -65dBm (+/-3dBm)

Installation Warnings:

- ➢ Don’t install the AP with the antenna pointing to a wall. That can potentially block the signal.
- ➢ Don’t install the AP in a metal enclosure. Metal blocks the signal.

- Don’t install the AP behind metal door (including an elevator) if the coverage area is on the other side of it.
- Don’t install the AP inside electrical boxes or closets. The AP needs to be clearly visible in the area it is supposed to cover.
- The AP is designed for indoor use only. Don’t install it in an outside setup.
- Don’t install the AP close to any microwave devices (MRI, microwave ovens, etc.), hence that will change the nature of the signal and affect the coverage.
- Do not spill water on the AP, it is not water resistant and that will damage it.
- Nonfood material, do not digest the USB AP.
- Keep away from children??

Antenna patterns:

The SH 2.0 USB uses two antennas to provide wireless connection with the monitoring devices/sensors. To do that the SH 2.0 USB AP connects with the Cisco Catalyst (need detail on the antenna specs here). For further detail on the antenna specifications see (CIsco Systems). The RTX3300 uses the 2 antennas on the Catalyst device using the so-called **fast antenna diversity**. That means that the RTX3300 dynamically chooses the best antenna signal based on its environment and uses that one.

NOTE: *Any enclosures may cage the signal and therefore it is important how we place the AP. For details on the proper placement of your USB AP see CH.XX*

Wireless Range

As we can see from the antenna patterns the wireless signal of the RTX3300 is not a spheric and all directional, but it is rather important how we place the USB AP for the direction of the signal to cover the areas that we will need coverage. Therefore, when we talk about wireless range, what we mean is the max distance we recommend the placement of USB APs from each other.

The wireless range of the RTX3300 USB AP are the following:

- Up to **XX m** indoors.

This range depends on the nature and quantity of any radio signal dependent items or materials in the installation site. The range can also be affected by any thick walls and other interference sources. Therefore, it is important to perform a proper site survey. Placing an extra AP should help you around signal barriers.

NOTE: *Follow the OTAS requirements and secure wide overlapping and redundancy.*

NOTE: *The RTX3300 is designed for indoor use only and therefore no outdoor range is specified.*

Planning OTAS topology

SH USB AP connects to the SH 2.0 System/network via the already installed Cisco Catalyst AP. That means the placement of the USB APs is already predetermined by the placement of the Wi-Fi APs. Nevertheless, a site survey is recommended, since OTAS limitations. That means, we might need to physically move some of the WiFi APs or rotate them to obtain a maximum quality of the signal.

- The RF and installation requirements of Cisco should be followed. For reference: Cisco Catalyst 9120/9130 deployment guides.

- The guidelines for installation of your USB AP and the RF requirements should be followed. For Antenna patterns and RF requirements please refer to the previous part of this chapter.
- Recommendation for topology and that there should be overlapping and backup

What to consider when planning OTAS topology:

- ✓ Link budget for redundancy: **-65dBm (+/-3dBm)** - to ensure uptime
- ✓ **Overlapping** – to ensure sync and no package loss

The main difference between using Philips SH 2.0 synchronization via the Sync Box and using *Over-the-Air Synchronization (OTAS)*, that we need to consider when planning our system, is that OTAS requires all APs to be able to see each other. That means ***OTAS requires higher density of access points***, because the antennas need to be in range in order to synchronize.

On the pictures/figures below is visually represented the difference in required density between SH 2.0 and the density of antennas necessary for OTAS. The coverage radius of the antennas/USB AP units is represented as a circle with the AP at its center. That is made for simplicity, the actual coverage area can be measured to be with an irregular shape. That is mostly because of the physical obstacles (walls, elevator shafts, electronic equipment that affects the propagation of radio waves) found in a hospital building. If we want our monitoring units to be able to roam without losing network connectivity in the desired area of coverage, we need to make sure those circles overlap in such a way that every USB AP is in the coverage radius of at least 2 neighboring AP units. That also secures us that in the cases where one of the units fails or stops functioning, the rest of the topology won't be affected and can continue functioning without delays and interruptions.

Fig.XX. Example of SH 2.0 Density

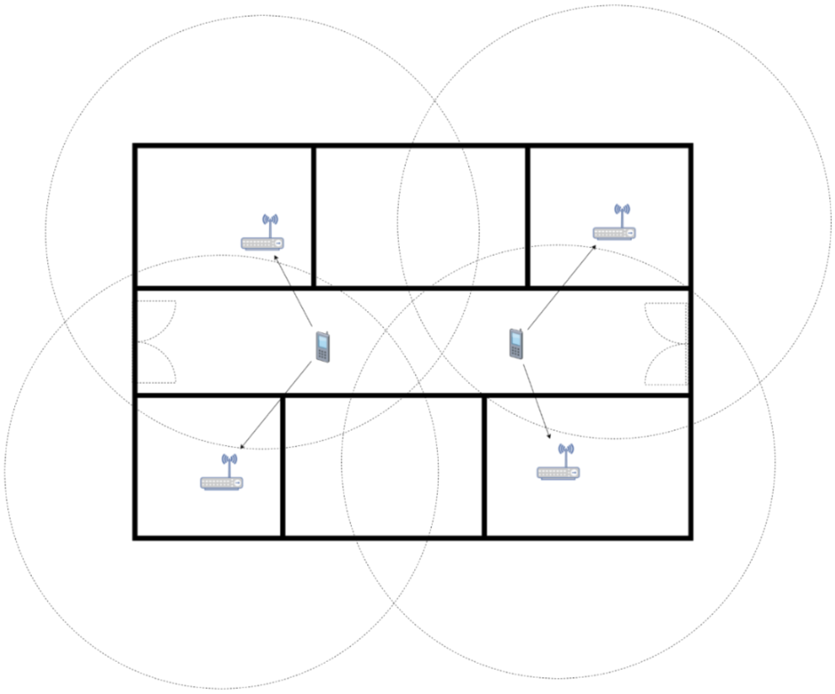
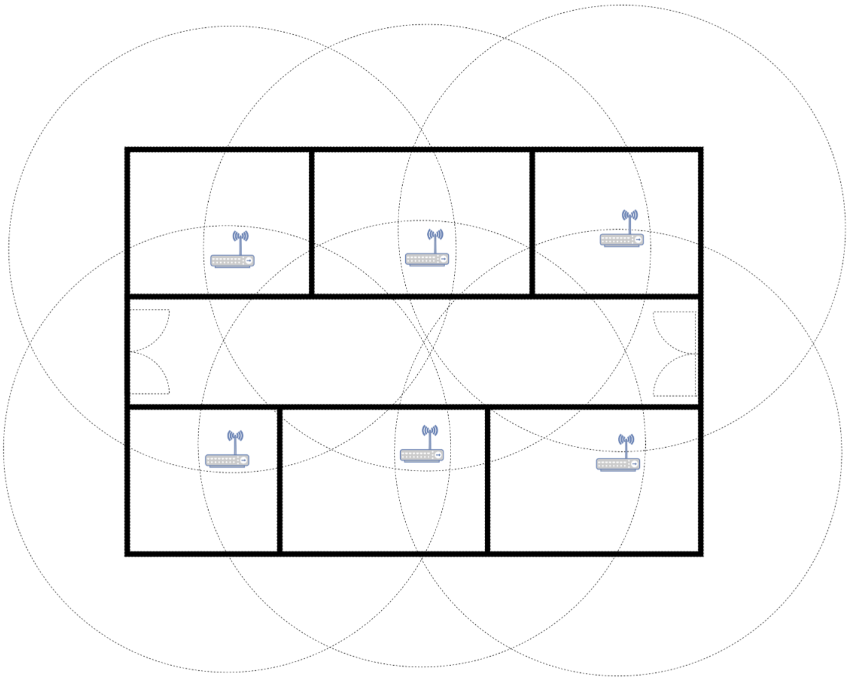


Fig.XX. Recommended OTAS Density



Site Planning

Make sure that before you start your deployment process you have done a proper site planning and considered the following:

- Determined the desired area of coverage withing the hospital.
- Determined the amount of USB AP necessary to provide that coverage.
- Plan the locations where those USB AP will be placed. If necessary, add additional units to satisfy the OTAS high density requirements.
- Plan your OTAS topologies.
- Define the number of APC needed to support your chosen topologies.
- Define the number of sync units (OTAS controller) required by your topologies.
- Perform a RF site survey.

Interference

As the SH 2.0 uses the frequencies between 1.4 GHz that are reserved for the Healthcare sector, there should not be interference from neighboring networks operating on the same frequency band to be considerate about. Nevertheless, it is recommended to double check beforehand.

Another factor that we need to be considerate about, as we plan our deployment, are the type of materials that the signal needs to go through (walls, etc.) Following table can give guidelines of the degree to which certain materials will obstruct the radio signal.

MATERIALS	DEGREE OF ATTENUATION	EXAMPLE
Air	None	Open space
Wood	Low	Floor, doors,
Plastic	Low	Cabinets, ??
Glass	Low	Windows and glass doors

Tinted Glass	Medium	Glass doors
Living Creatures	Medium	Plants, crowds
Bricks	Medium	Walls
Ceramic	High	Tiles
Concrete	High	Walls, floors/ceilings, pillars, stairs
Metal	Very high	Metal cabinets, metal plated doors, columns, elevators, metal framed beds?

Table XX Radio Attenuation for different materials

Deployment process

Each installation side is different even if it is part of the same hospital chain or designed with the same plan. It is a good practice to create a site map to identify the best locations to mount your SH USB APs. It is a good idea to supply yourself with the building plans, that will help you pinpoint the RF attenuation materials and RF interference sources on your site map.

The SH 2.0 USB AP can provide indoors coverage of approx. **XX m (XX feet)** depending on the building materials and interference sources.

Among others the number of users, traffic density, or where we need coverage, should be considered beforehand when planning the placement of your USB APs. When deciding the location of APs, prioritize the areas where the patients spend most of their time. Make sure you use an up-to-date floor plan.

To perform your site survey, you will need Philips Site Survey Toolkit.

Table with installed units for user to fill in with IP addresses and position of the APs

Nr	AP's MAC address	IP ADDRESS	PHYSICAL PLACEMENT
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

NOTE: *When performing a site survey in a healthcare setting it is important to remember that there are a couple of special considerations that need to be recognized or they will alter the survey results. For example,* *hospitals may have management spaces (basically another floor between floors) that are used to run various patient support systems to bed locations. Another special consideration is that radiology departments commonly have containment shielding for systems such as MRIs, and extensive steel or concrete support structures.*

Start by placing your first USB Access Point considering the areas that need to be covered by the signal. This will be easier if you already have a plan of the building with appointed all the places with installed WIFI Catalyst Access Points. Then measure the signal strength all around the area we are installing it in and at –65dBm install your second access point. If the planning process has been done properly, there should be already present a Wi-Fi AP in the area we want to install it. Therefore, it is very important to plan your OTAS topology beforehand and install your WIFI APs with this prerequisite in consideration. Installing a new Cisco WLAN network for the purpose of building a WMTS system allows us to plan our WLAN in a way that will serve also the purposes of the ITS (IntelliVue Telemetry System).

Keep installing your USB APs in the same manner until all the desired area is covered.

Picture of coverage examples. Pictures of proper placement of USB AP.

Table of AP placement, IPs and RSSI.

Ends with: next steps will be installing this and that and ref. to the pages with instruction for installation

Deployment Scenarios

We have overseen the following deployment scenarios:

- Deployment of pure USB AP infrastructure on new Cisco Wi-Fi AP infrastructure.
- Deployment of pure USB AP infrastructure om existing Cisco Wi-Fi AP infrastructure
- Deployment of mixed SH2.0 and SH USB AP infrastructure
- Extension of existing SH infrastructure with additional USB APs to extend coverage. (To be discussed in appendix?)

1 Deployment planning of pure USB AP infrastructure on new Cisco Wi-Fi AP infrastructure

If you are setting up your Cisco network with the plan to implement an SH USB AP infrastructure on it bear in mind the following:

All Cisco AP need to be placed with the consideration that there will be an SH USB AP mounted on them. That means **the USB port on the Cisco Catalyst AP needs to be accessible.**

The SH 2.0 USB AP needs to be pointed to the room. Any wall and ceiling represent a physical barrier for the radio signal and will interfere with the proper functionality of your SH 2.0 USB AP system.

Need to make sure that your WLAN access points are placed along the desired coverage area to provide signals from multiple angles and to make sure that the SH USB AP can ‘see’ each other. That is required because the SH USP AP uses Over-The-Air Synchronization and in order to synchronize units a higher density is necessary.

~~***NOTE:*** *When performing a site survey in a healthcare setting it is important to remember that there are a couple of special considerations that need to be recognized or they will alter the survey results. For example,*~~

~~*hospitals may have management spaces (basically another floor between floors) that are used to run various patient support systems to bed locations. Another special consideration is that radiology departments commonly have containment shielding for systems such as MRIs, and extensive steel or concrete support structures.*~~

For details on planning your WLAN deployment refer to the ***Cisco WLAN Deployment Guide for Healthcare.***

Allowed and prohibited AP positions.: When mounting your USB AP bear in mind the AP needs to point to the room. Any wall or ceiling presents a physical obstacle for the signal and will interfere with the normal operation of the device.

The site survey should have been made already by Cisco and Philips; however, we recommend you make your own and have a tool for measuring the signal strength when installing your SH USB Devices on the Wi-Fi Access points. As mentioned, that is required because OTAS needs higher density of the APs. It would be also a good practice to be aware beforehand of the possible interference sources and try to simulate those as you install your units. That will allow you correct the position the APs if necessary already upon installation and prevent future disturbances of the seamless work of the system.

2. Deployment planning of pure USB AP infrastructure on existing Cisco Wi-Fi AP infrastructure

3. Deployment of mixed SH2.0 and SH USB AP infrastructure

Expanding and modifying an existing network

Adding more APs to already existing zone of APs

Site Verification

Ends with: how to see that everything works ok? Site verification

Refer to philips

OTAS: RF & sync

Chapter 3: Installing and Configuring your SH USB AP

This chapter will guide you through the installation process and assist you in setting up a working patient monitoring system.

Overview of the procedure

The following procedure describes the steps you need to follow in order to successfully install your 2.0 SH USB Access point and configure and setup your SH infrastructure.

Required prerequisites:

- An existing SH 2.0 infrastructure with PIIC and APC, installed according to the applicable Philips documentation
- Installed and configured IOx application via DNA Center. It needs to be deployed to all Cisco APs where SH AP is installed. Once the IOx software package has been deployed and configured, the USB AP will be connected to the AP Host and be visible in the Access-Point Controller (APC) Web Page.
- IP Address of the AP host needs to be configured in the application configuration provided via the application deployment tool in the DNA center
- Wireless LAN Controller has to be configured and have a site setup.

Steps of installation (and configuration):

Step 1 Install AP Host software and configure it to work with the SH USB AP.
Step 2 Make sure the Wireless LAN Controller (WLC) has a site setup.
Step 3 The DNA Center must have the same site set up
Step 4 Connect your Cisco Catalyst AP to your LAN.
Step 5 Mount your SH USB AP on the Cisco Catalyst AP.
Step 6 Deploy the SH 2.0 IOx Application to the Cisco DNA Center and provision it to the AP on the relevant site.
Step 7 Configure your APs to look at the IP of the AP Host.
Step 8 Connect the Cisco AP to the site in the WLC.
Step 9 AP Host automatically generates a Virtual Access Point (VAP) in Docker.
Step 10 On AP Host run “Docker container ls” command to verify that VAP is present.
Step 11 Run command “Docker container inspect <name of the VAP>”
Step 12 In the information that comes up from last step look for MAC address matching the SH USB AP
Step 13 Locate in APC the VAP corresponding to the physical SH USB AP. That allows us to add it to an AP group.

Configuration of the AP Host for USB AP

Specifications for the AP Host:

AP-host machine model: P350

Specs:

Lenovo ThinkStation P350 30E3 - Tower - 1 x Core i7 11700K / 3.6 GHz - vPro - RAM 32 GB - SSD 512 GB - TCG Opal Encryption, NVMe - T1000 - GigE - Wi.

Linux configuration: Ubuntu server with SSH enabled

NOTE: *Your AP Host PC is going to need two LAN cards, because it needs to be connected to both the Philips Supplied Network and the Management network/Customer Supplied Network simultaneously.*

NOTE: *AP Host must have static IP addresses: Both the Relay app and the ini-file below statically denote the AP Host IP, so both Relay and OTAS fail if the IP changes.*

NOTE: *You must create a vap.ini-file on AP Host at /opt/rtx3300/vap.ini containing the below lines:*

```
[otas]
otasIP=<IP of APHost running OTAS>
otasPort=9000
```

That is a necessary part of the initial configuration of the AP Host device. The vap.ini-file is pointing to the AP Host machine currently running the OTAS software and to the proper port it connects to.

To install and configure your AP Host follow the steps:

1. First you need to update your Ubuntu server if it is not up to date. You do that depending on the version following the responding procedures.
2. Next step is to install **Net-tools**. That is a collection of programs for controlling the network subsystem of the Linux kernel. This is required, to gather the required network information (MAC addresses) and view/sync with the general network interface configurations. ~~because that will make it easier to display the different interfaces and run the desired commands~~.
3. You are going to need Docker on your Ubuntu server to contain the VAPs. To check if there is Docker installed you can use the command: "$ docker version ". If Docker version information is displayed on the screen, there is Docker installed. Elsewhere, you need to install Docker. You can do that by following the steps here: https://docs.docker.com/engine/install/ubuntu/
4. To configure your Ubuntu machine to work better with Docker, follow the post installation instructions here: https://docs.docker.com/engine/install/linux-postinstall/#manage-docker-as-a-non-root-user
5. Once you have installed and configured Docker on your Ubuntu server PC you need to check if there is an existing mcvlan network. That is the network that will handle the creation of VAP in Docker.

We can check for its existence with the command: "*$ docker network ls*" and look for a network called **my-macvlan-net-2.** That is the name that is hard coded in the APC and therefore it is essential we do not change that. If the network does not exist, you need to create it by using the command:

```
docker network create -d macvlan \

  --subnet=172.31.24.11/21 \

  --gateway=172.31.27.0 \

  --ip-range=172.31.26.128/25 \

  -o parent=enp1s0 \

 my-macvlan-net-2
```

This configuration is done to tell Docker what network it should look to for the MAC addresses for the VAP it will create.

The *subnet* and *gateway* are acquired by your network administrator.

It is very important that we define the *ip-range* in the AP Host, in order to avoid any conflicts with the SH 2.0 APs in the system. That is why we should define a unique subrange from IP range from the reserved from Philips. For more details on that please refer to the ***RTX3300 Network planning guide***.

6. Next step is to install the RTX software that will configure our Ubuntu server PC to be able to host virtual access points (VAP).
7. You need to copy the file to your Ubuntu server PC and unzip the file using the appropriate commands (those may vary depending on your software version). You can deliver the files to the Ubuntu server PC via external HDD.
8. Once you unzip the file, load docker images. Run the install.sh executable file that will configure the Ubuntu server PC to host our Virtual Access Points (VAP).
9. The last step is to connect the second network cable/card to the Management network.

Your AP host is now configured to service your VAP units.

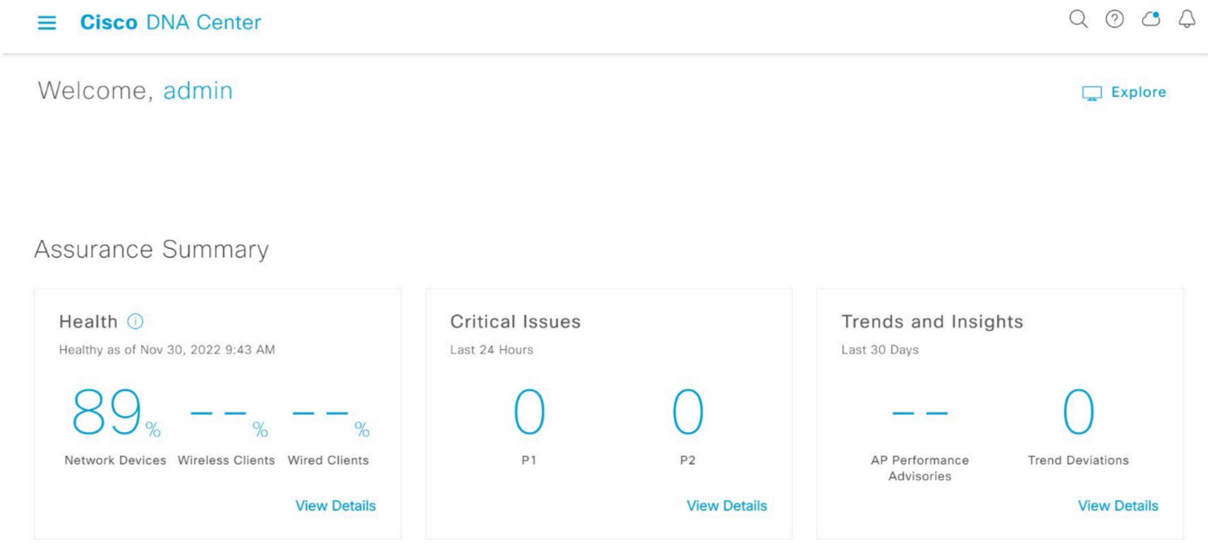
Known limitations:

- VAP and OTAS Container must run on the same host.
- VAP and OTAS Container must be started manually.
- OTAS sync sources must be provided at the command line when OTAS is started.

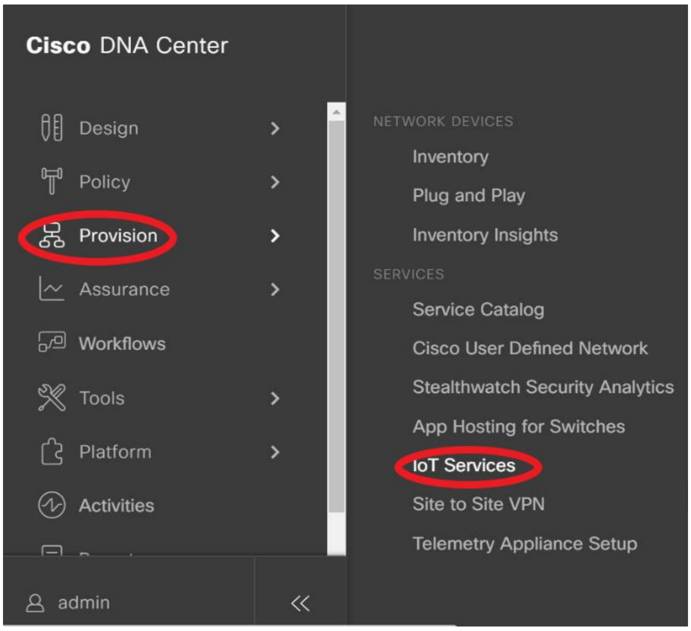
Installation and configuration of the IOx Application

This subchapter contains a step-by-step guide on provisioning your IOx Application software on the Cisco Catalyst AP through the Cisco DNA Center (step 6 from the whole procedure).

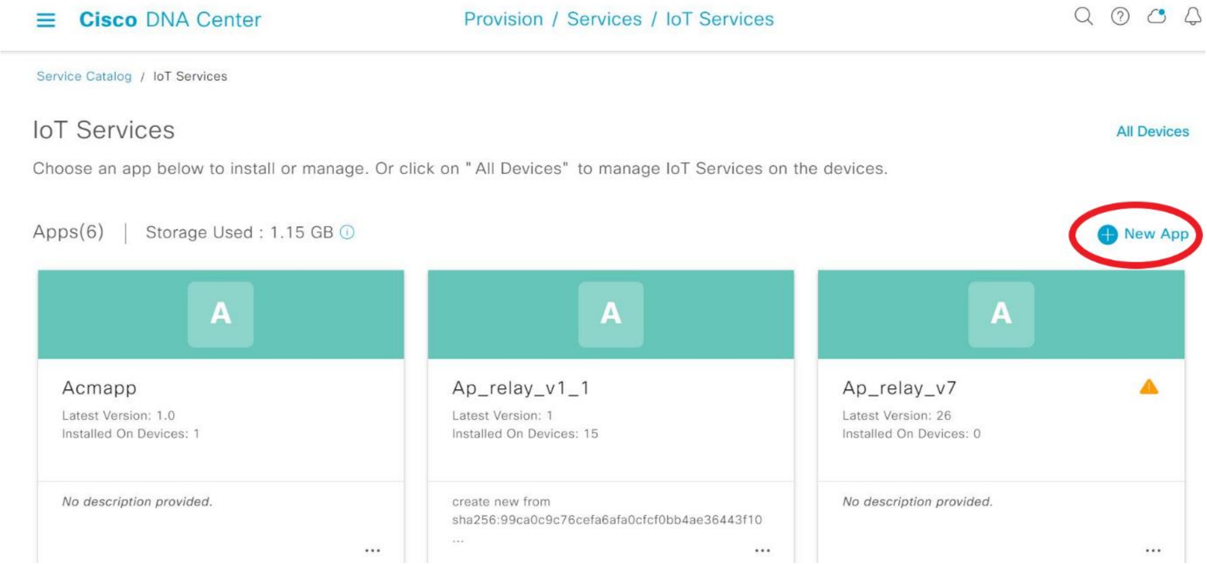
Step 1 Log in the DNA center



Step 2 Open the menu ☰ and choose **Provision > IoT services**



Step 3 There you can see the apps that are ready to install. If the app you are looking for is not already there you can always upload it from your computer. Just press on **New App**:


Cisco DNA Center
Provision / Services / IoT Services
Service Catalog / IoT Services
All Devices
New App
A
A
A
...
...
...

IoT Services

Choose an app below to install or manage. Or click on " All Devices" to manage IoT Services on the devices.

Apps(6) | Storage Used : 1.15 GB

Acmapp
Latest Version: 1.0
Installed On Devices: 1

No description provided.

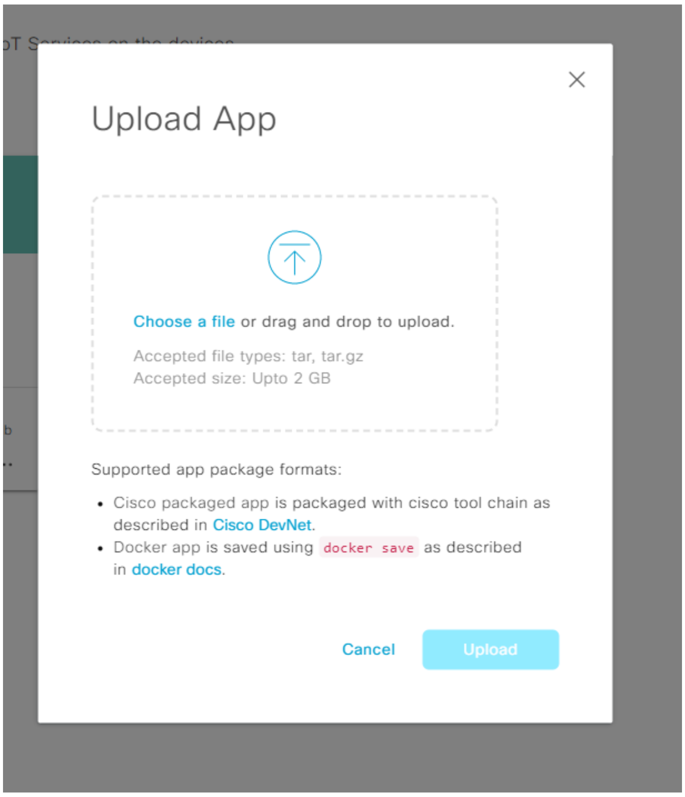
Ap_relay_v1_1
Latest Version: 1
Installed On Devices: 15

create new from
sha256:99ca0c9c76cefa6afa0cfcf0bb4ae36443f10
...

Ap_relay_v7
Latest Version: 26
Installed On Devices: 0

No description provided.

Step 4 You can drag and drop your exe. file or upload it by pressing the **Upload** button:



Upload App

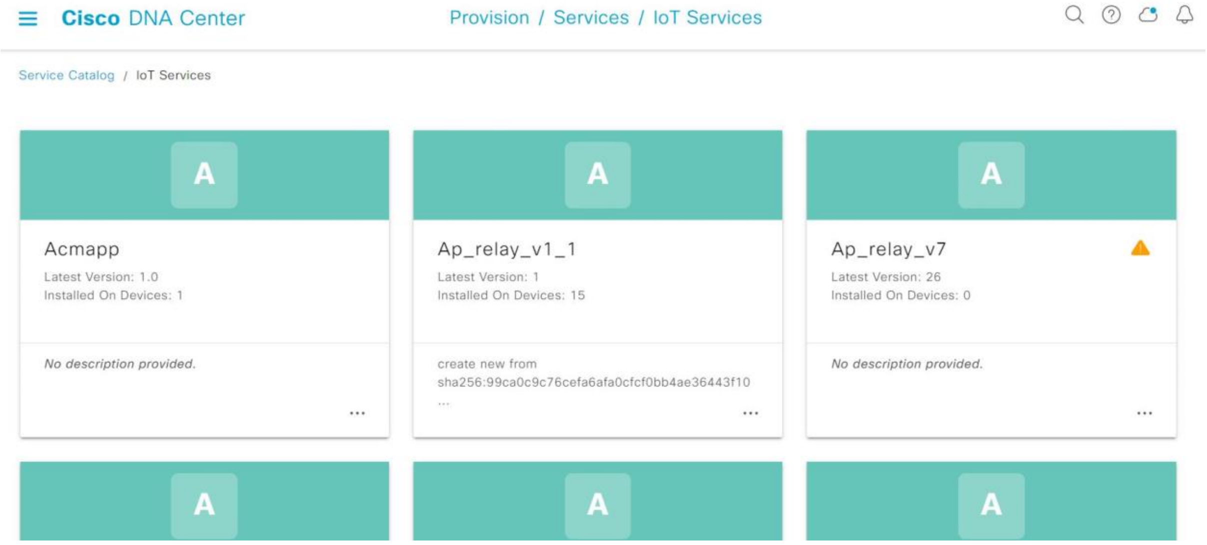
Choose a file or drag and drop to upload.

Accepted file types: tar, tar.gz
Accepted size: Upto 2 GB

Supported app package formats:

- Cisco packaged app is packaged with cisco tool chain as described in Cisco DevNet.
- Docker app is saved using `docker save` as described in docker docs.

Step 5 Choose the app to install and click (once) on it.



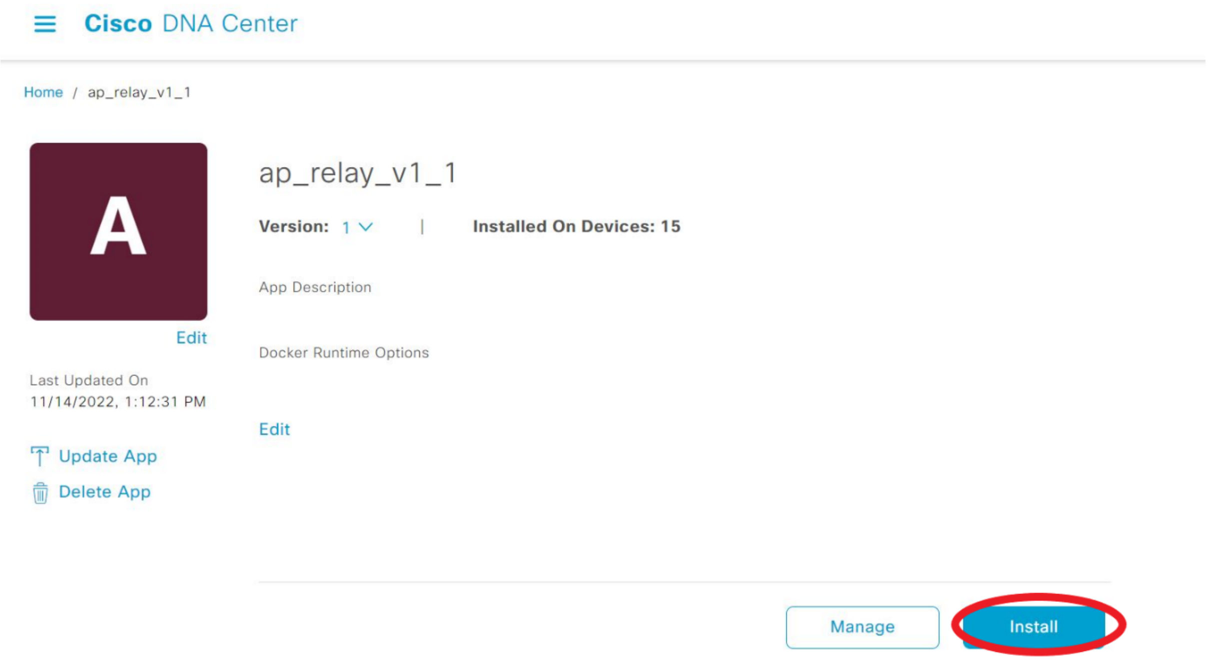
Cisco DNA Center
Provision / Services / IoT Services
Service Catalog / IoT Services
A
A
A
A
A
A

Acmapp
Latest Version: 1.0
Installed On Devices: 1
No description provided.

Ap_relay_v1_1
Latest Version: 1
Installed On Devices: 15
create new from sha256:99ca0c9c76cefa6afa0cfcf0bb4ae36443f10 ...

Ap_relay_v7
Latest Version: 26
Installed On Devices: 0
No description provided.

Step 6 It opens the page with the app functions and then you can press **Install**:



Cisco DNA Center

Home / ap_relay_v1_1

ap_relay_v1_1

Version: 1 | **Installed On Devices: 15**

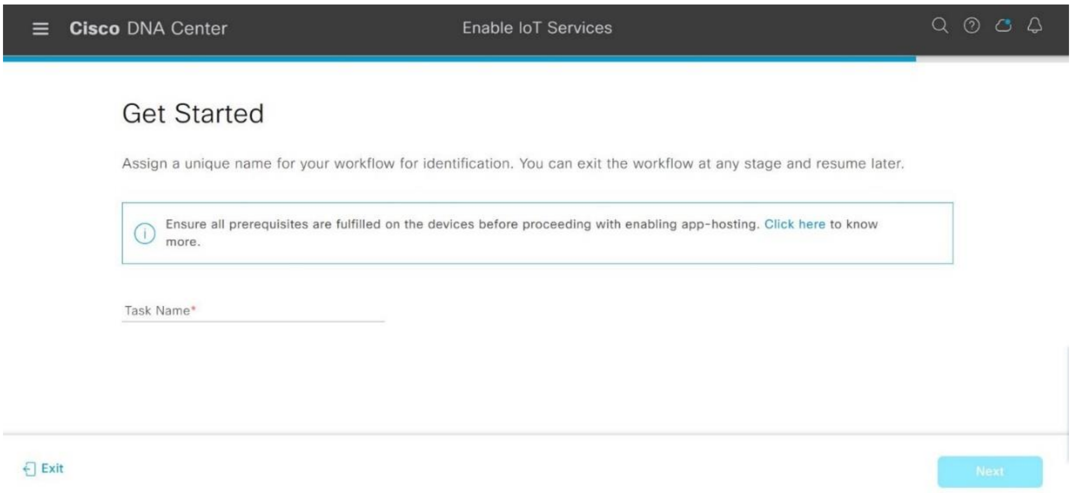
App Description

Docker Runtime Options

Edit

Last Updated On
11/14/2022, 1:12:31 PM

Step 7 Give a name to your task and click **Next**:



Cisco DNA Center — Enable IoT Services

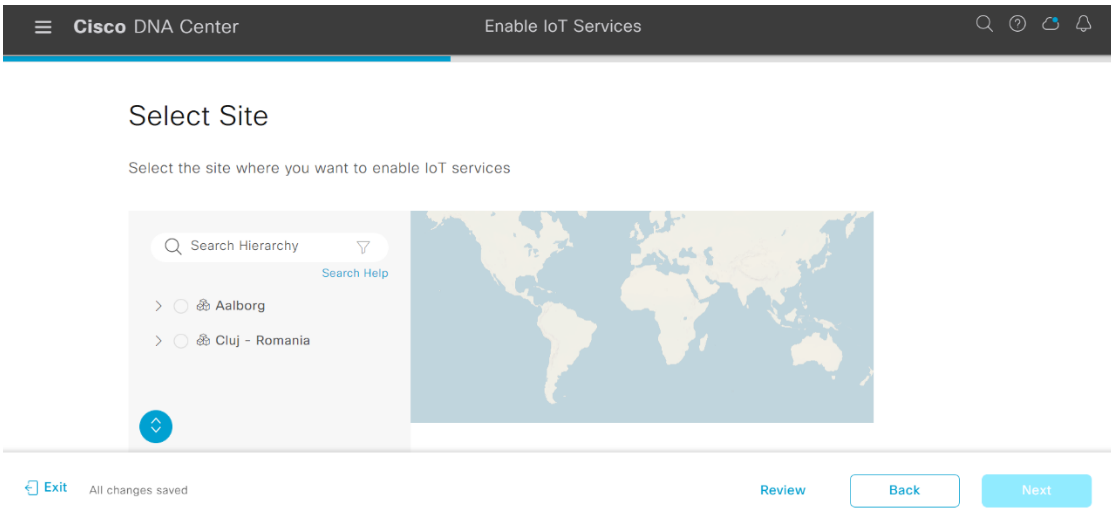
Get Started

Assign a unique name for your workflow for identification. You can exit the workflow at any stage and resume later.

Ensure all prerequisites are fulfilled on the devices before proceeding with enabling app-hosting. Click here to know more.

Task Name*

Step 8 Select the site where your device is installed and click **Next**:

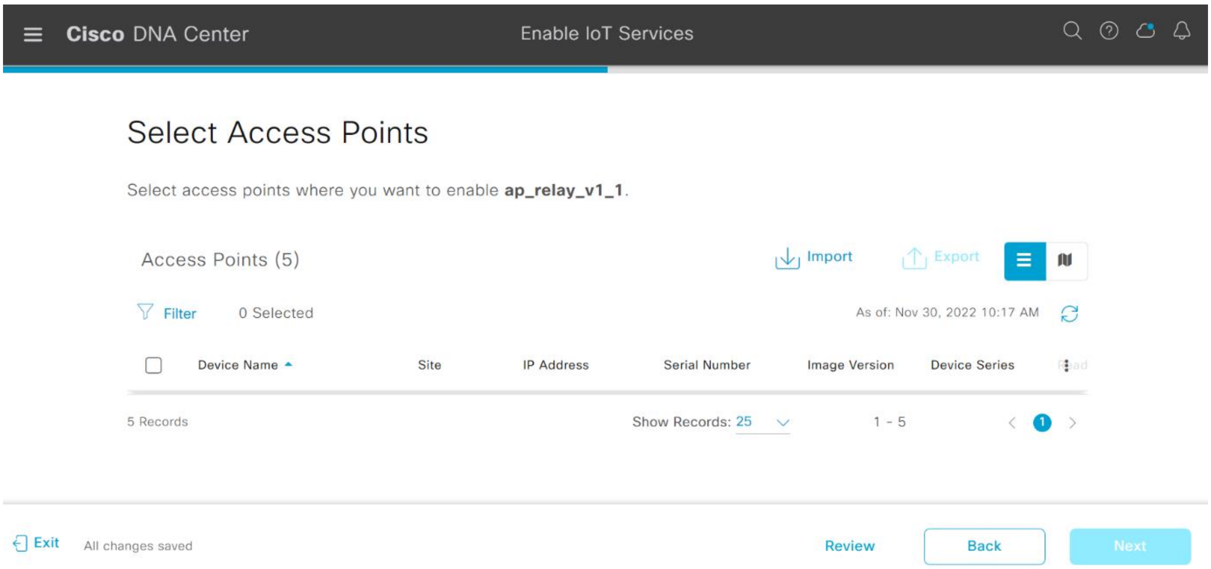


Cisco DNA Center — Enable IoT Services

Select Site

Select the site where you want to enable IoT services

Step 9 Select AP you want to install your IOx application on. It could be one at a time and multiple at once. And then press **Next**. If your screen isn't big enough might occur that you are not able to see the list of devices:



Cisco DNA Center — Enable IoT Services

Select Access Points

Select access points where you want to enable **ap_relay_v1_1**.

Access Points (5)

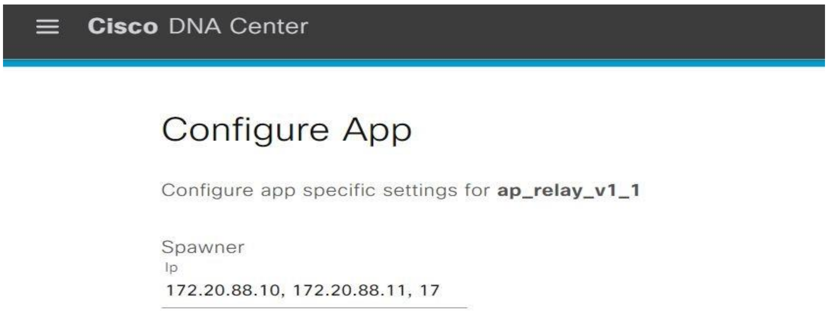
Filter 0 Selected As of: Nov 30, 2022 10:17 AM

□	Device Name	Site	IP Address	Serial Number	Image Version	Device Series

5 Records Show Records: 25 1 - 5

Step 10 Here we have to log the IPs for the AP Host, because that is where the VAP corresponding to our AP is created. IOx Application oversees both aiding the Cisco Catalyst in recognizing the SH USB AP and connecting it to the AP Host, so the AP host can create a VAP.

Configure app specific settings for the IOx application and click **Next**:



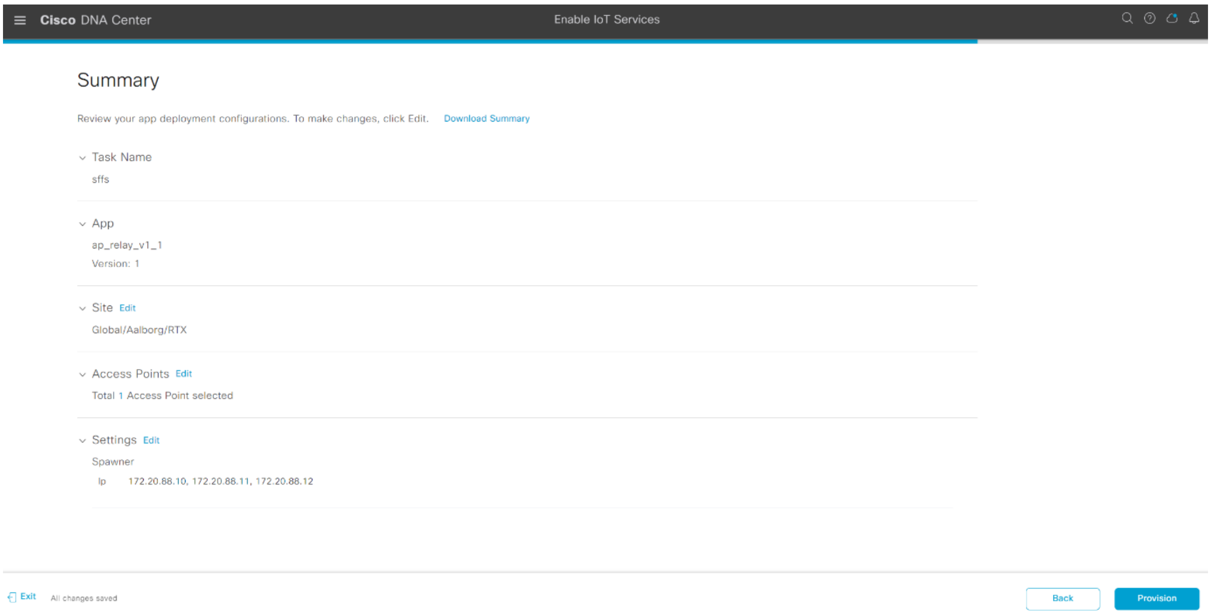
Cisco DNA Center

Configure App

Configure app specific settings for **ap_relay_v1_1**

Spawner
Ip
172.20.88.10, 172.20.88.11, 17

Step 11 Now you can see on the screen a summary of all your configuration so far. If everything looks right press **Provision** and go ahead with the installation.



Summary

Review your app deployment configurations. To make changes, click Edit. Download Summary

Task Name
sffs

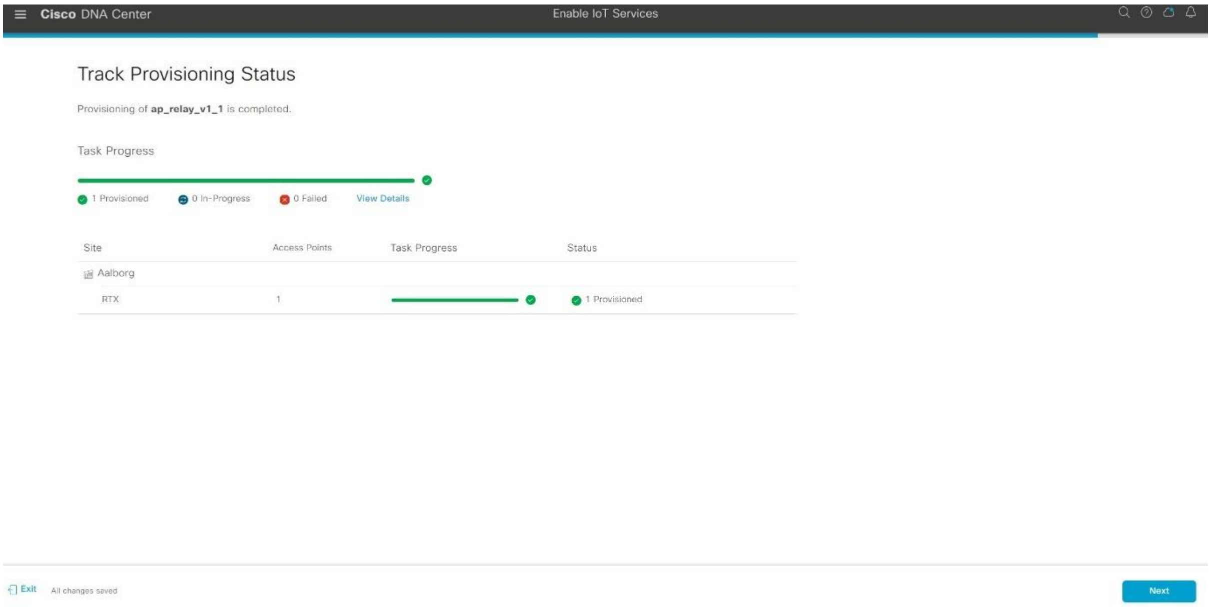
App
ap_relay_v1_1
Version: 1

Site Edit
Global/Aalborg/RTX

Access Points Edit
Total 1 Access Point selected

Settings Edit
Spawner
Ip 172.20.88.10, 172.20.88.11, 172.20.88.12

Step 12 You should be able to see the status of the installation:



Track Provisioning Status

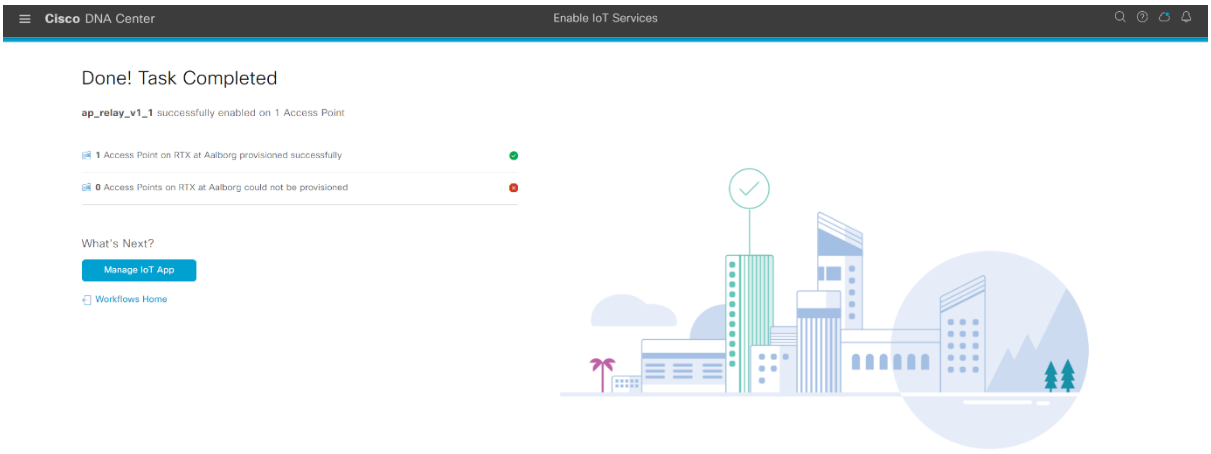
Provisioning of **ap_relay_v1_1** is completed.

Task Progress

1 Provisioned 0 In-Progress 0 Failed View Details

Site	Access Points	Task Progress	Status
Aalborg			
RTX	1		1 Provisioned

Step 13 When it is done provisioning the IOx to the AP we can press **Next,** and the installation is done.



Done! Task Completed

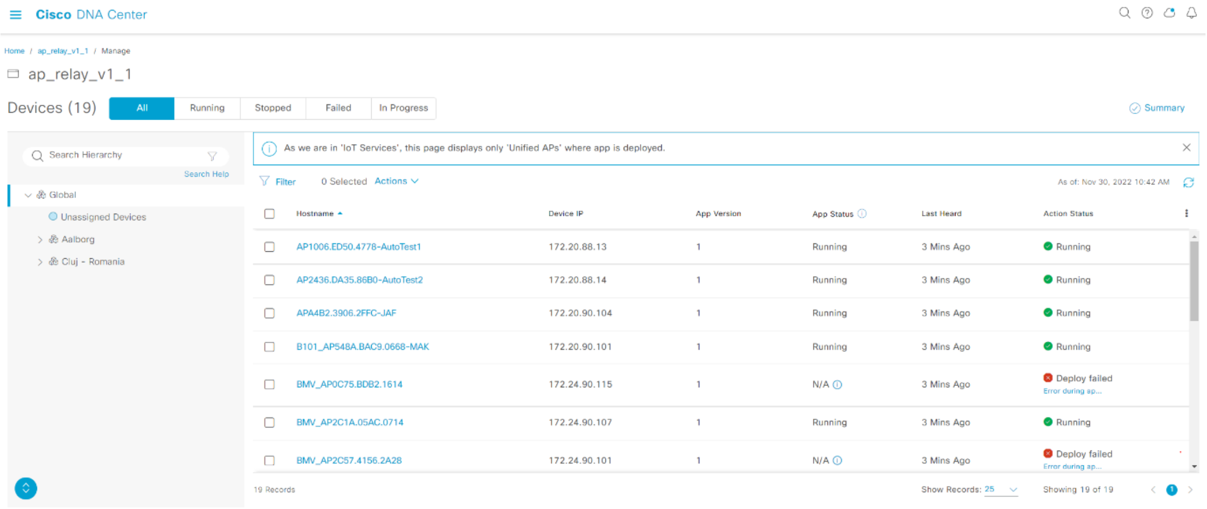
ap_relay_v1_1 successfully enabled on 1 Access Point

1 Access Point on RTX at Aalborg provisioned successfully ✓

0 Access Points on RTX at Aalborg could not be provisioned ☒

What's Next?

Step 14 If we press Manage IoT App we can see the status of all our devices:



As we are in 'IoT Services', this page displays only 'Unified APs' where app is deployed.

As of: Nov 30, 2022 10:42 AM

□	Hostname	Device IP	App Version	App Status	Last Heard	Action Status
□	AP1006.ED50.4778-AutoTest1	172.20.88.13	1	Running	3 Mins Ago	● Running
□	AP2436.DA35.86B0-AutoTest2	172.20.88.14	1	Running	3 Mins Ago	● Running
□	APA4B2.3906.2FFC-JAF	172.20.90.104	1	Running	3 Mins Ago	● Running
□	B101_AP548A.BAC9.0668-MAK	172.20.90.101	1	Running	3 Mins Ago	● Running
□	BMV_AP0C75.BDB2.1614	172.24.90.115	1	N/A	3 Mins Ago	☒ Deploy failed Error during ap...
□	BMV_AP2C1A.05AC.0714	172.24.90.107	1	Running	3 Mins Ago	● Running
□	BMV_AP2C57.4156.2A28	172.24.90.101	1	N/A	3 Mins Ago	☒ Deploy failed Error during ap...

19 Records

Show Records: 25

Showing 19 of 19

For further details refer to Cisco's DNA Center guide: Cisco DNA Center - End-User Guides - Cisco

Mounting the USB

This subchapter will present a step-by-step guide of how to mount your USB AP onto the Cisco Catalyst AP

Things to consider beforehand:

1) How is the Cisco Catalyst Wi-Fi AP mounted? Check if the USB port is accessible.
   If the Cisco Wi-Fi AP is mounted in metal enclosure (from Oberon or AccelTex) you need to take the Wi-Fi AP out of the enclosure in order to install the USB AP. Bear in mind that after mounting the USB AP on the Cisco AP, the module might not be fitting in the metal enclosure anymore.
2) Should be below ceiling, metal net on ceiling can become an obstacle for the signal
3) When installing on walls should be considered that walls are physical obstacles to the wireless signal

Contents of the package:

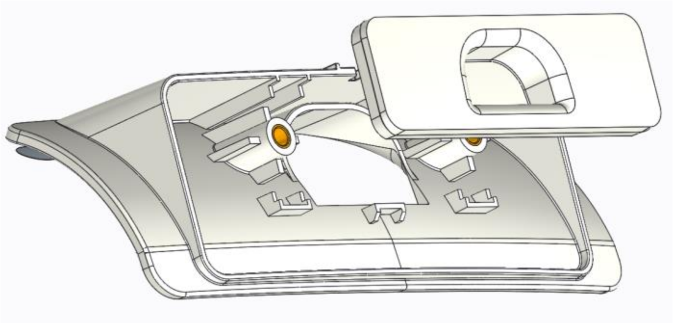
USB AP, secure bracket, dummy USB, tightening tool

Designed for interior environment the USB AP should be used only in indoor, hospital-like environments. Once Installed the USB AP should not be removed. A simple user interface is provided by 1 RGB LED.

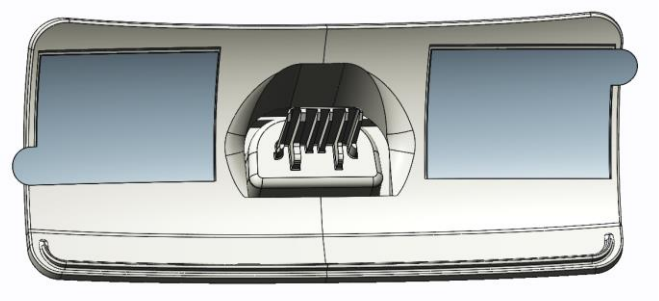
Before you install the USB AP on your Cisco Catalyst AP, you need to fix the Bracket at the Wi-Fi Access Pont. That can be done in the following manner:

Step 1 Remove the cap from the USB port on your Cisco Catalyst AP.

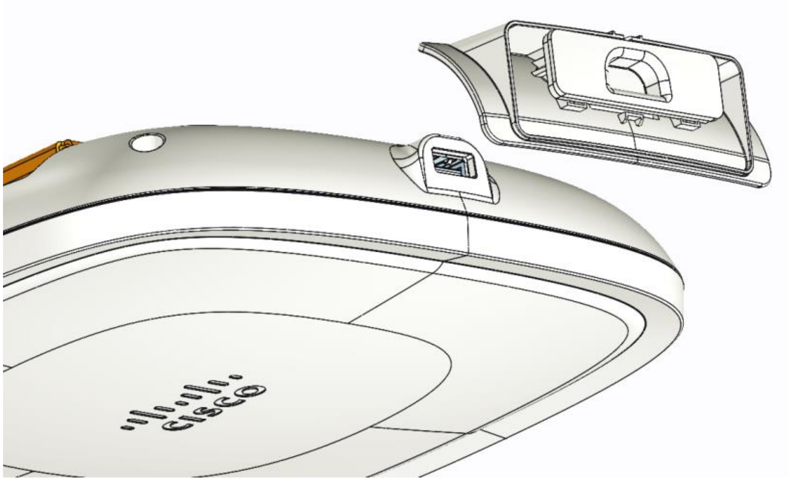
Step 2 Install the Dummy USB to the Bracket.



Step 2 Peel off the protection foil on double-sided tape at the backside of the bracket.



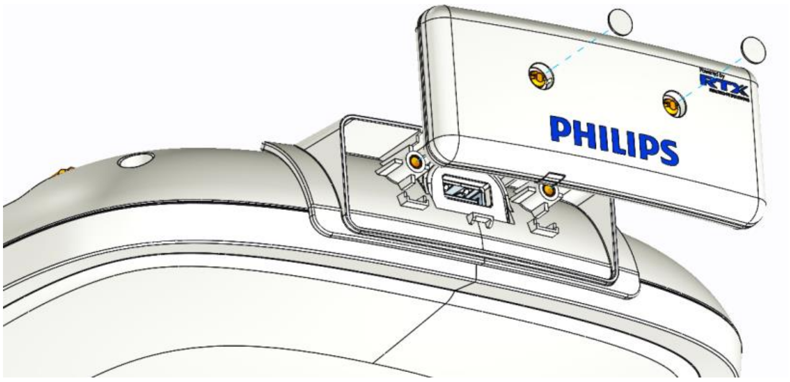
Step 3 Insert the Dummy USB together with the bracket into the USB port of the Cisco AP.



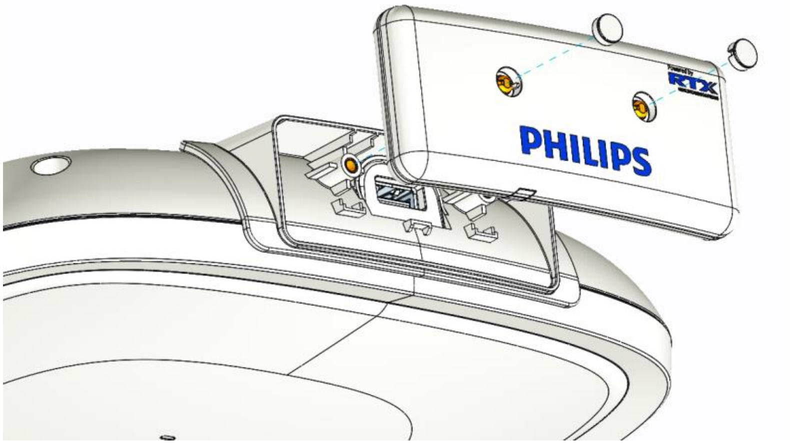
Step 4 Press firmly to ensure the bracket is well mounted on the Cisco Catalyst AP.

Step 5 Remove the Dummy USB from the USB port.

Step 6 Insert the USB AP into the USB port of the WiFI AP and tighten the screws with the provided tool.



Lastly insert 2 pcs of screw covers provided onto the USB AP's plastic casing. That is important to ensure protection from electrostatic discharges.



The secure tamper-proof mounting bracket/interlock is designed, to avoid the AP to be removed intentionally or unintentionally. Removing the USB AP will compromise the proper functioning of your WMTS Smart-Hopping Patient monitoring system.

Chapter 4: Interaction with the PiC iX

OTAS interacts with the PiC iX UI just as the SH 2.0 does and is able to send alarms to it. When OTAS alarm is generated, it is forwarded from the OTAS controller to the Philips Alert Server and to the PiC iX UI.

The alarms are first sent to the VAP instance which then sends to the alert server like any other alarm from the AP. The alarms shall show the ID of the AP, if specified by the OTAS controller. The ID shall be shown so that the user can easily correlate with the IDs shown on APC and OTAS controller status web page on the AP Host (MAC, IP address, possibly FMID).

OTAS-specific alarms are not yet specified in the alert server (no specific alert/alarm identifiers have been assigned). For the time being, we use the APWMTS_ALERT_RAA_FAILED (0x8F11) as a placeholder for all OTAS-related alarms. The alarm includes a value (which shown on alert server) that is used to indicate the specific OTAS alarm according to the table below.

It is expected that the OTAS alarms will be changed to become individual alert identifiers at some later time.

Table with all the new alarms coming from OTAS and USB AP.

ALARM ID	NAME	DESCRIPTION
0	OTAS_ALARM_TYPE_INITIAL_SEARCHING_LONG	WARNING/CLEAR, while booting (autonomous tree generation). CLEAR in locked state. Initial search state is taking longer than expected. Some APs may be out of service or RF conditions may be poor.
1	OTAS_ALARM_TYPE_INITIAL_MASTER_CAND_SEARCHING_LONG	WARNING/CLEAR, while booting (autonomous tree generation). CLEAR in locked state. Initial search state is taking longer than expected. Some APs may be out of service or RF conditions may be poor.
2	OTAS_ALARM_TYPE_BAD_TREE_LINK	ERROR/CLEAR, if a link in tree is worse than threshold. Whenever a "good" tree is calculated, we set a clear event. A tree is active, but one or more links have worse RSSI than set warning threshold. Check tree and AP service state.
3	OTAS_ALARM_TYPE_TREE_TOO_MANY_LEVELS	ERROR/CLEAR, if a tree contains too many levels. A tree is active, but maximum depth exceeds warning threshold. Check AP service states and primary/secondary selection for options to reduce tree depth.
4	OTAS_ALARM_TYPE_ISLAND	CRITICAL/CLEAR, after island is generated (action needed to recover) A subtree has detached from the main tree and is now free running. The subtree will not automatically resync with main tree and roaming between main tree and detached branch will not be possible. Review sync tree and AP service state. Restart APs in subtree to recover.

5	OTAS_ALARM_TYPE_EXTERNAL_ISLAND	CRITICAL/CLEAR, after alien island is generated, when sync is lost to external sync source (action needed to recover) The sync tree has lost synchronization to external sync (fixed SH AP). Restart all APs to recover.
6	OTAS_ALARM_TYPE_LOOSING_SYNC	WARNING/CLEAR, when in FREE_RUNNING, ASSISTED_LOCK. CLEAR in locked state. An AP has lost synchronization and become free running. Will eventually detach from main sync tree and become unrecoverable.
7	OTAS_ALARM_TYPE_NO_TREE_REDUNDANCY	ERROR/CLEAR, when there is no redundancy in tree (may be caused by AP fw update or controlled AP power cycle). CLEAR if redundancy calculation shows no issue. A tree is active, but there is insufficient redundancy in tree to recover from single point of failure. Review AP service state and RF conditions.
8	OTAS_ALARM_TYPE_ALIEN_SEARCHING_LONG	WARNING/CLEAR, while searching for alien sync source. CLEAR in alien locked state. Search for external sync source (fixed SH AP) taking longer that warning-threshold.
9	OTAS_ALARM_TYPE_ALIEN_LOOSING_SYNC	WARNING/CLEAR, when in ALIEN_FREE_RUNNING. CLEAR in alien locked state. A primary/secondary AP has lost synchronization to external sync source (fixed SH AP). Will eventually lose ability to recover. Check fixed AP service state and RF conditions.
10	OTAS_ALARM_TYPE_UNSTABLE	Not in first delivery: WARNING, if calculated tree various too much over time. The OTAS controller is reconfiguring the tree very often, due to unstable links between APs. Check AP uptime and RF conditions.

Please note that the currently used alarm ID is a placeholder, because the server is not updated with the new OTAS alarm. The user will need to know that these are OTAS alarms.

The FMID/MAC/IP Address of the AP(s) generating the alert is not currently shown on the alert server. This is a known bug.

Chapter 5: Troubleshooting

Synchronization procedures (OTAS?)

OTAS alarms related to topology issues and mismatches.

-'**no redundancy' alarm**: shows that the system is currently running but it's critical, in the meaning of if one unit falls out that will affect multiple units in the tree. Appropriate action here is to choose another structure of the tree.

Troubleshooting known issues

Alert explanations, warnings, and error messages

Maybe a table with what do they mean?

Troublehooting using the LED

What to do when a unit needs replacement: procedure, how to replace it and where to order a new unit from.

If we need to replace AP might need reconfiguration of the OTAS tree, if replacing primary or secondary sync source

Tools for troubleshooting? (Upgrading tool, assessment tool, statistics)

Philips Upgrader tool?

For issues with Philips Upgrader Tool refer to…

Cisco DNA Center?

For issues with Cisco DNA Center please refer to...

Chapter 6: System Update

This chapter describes the process of updating the different parts of the system.

Update Prerequisites:

- ✓ Installed Philips Upgrader tool on a service PC?? following the instructions in ref.
- ✓ Connect the service PC?? to the SH 2.0 system/infrastructure subnet
- ✓ Create/Export a backup of the current configuration in case of unexpected outcomes during updating. There should be a backup in OTAS configuration in AP Host.
- ✓ Before updating any Cisco units, check compatibility list (add reference) with USB APs
- ✓ Plan your procedure with the consideration of the proper order of updating the different parts of the system.
- ✓ Upgrade IOx application via DNAC

When we need to update USB APs and APC, we should upgrade APC first and then USB APs.

When we need to update multiple USB APs, bear in mind that your system will need to reboot and will be out of service for a period of time (between xx and xx min). That means you need to do that in a time when there are enough personnel in the hospital to monitor the patients and be able to react, if necessary, while the system reboots. (Also, in a time when patients are not roaming.)

Update all APs in a zone at the same time?

To guarantee proper functioning of your SH 2.0 all parts of the system need to be the same/corresponding software versions.

List of versions (or higher) of the components that work with SH 2.0 USB AP:

APC – D.02 software

AP Host – Ubuntu 20.04

Cisco – for later (refr to online compatibility matrix?)

Cisco

DNA center

Refer to documents:

Philips Upgrader tool

Software updated

Refer to the documents:

Upgrading IntelliVue Smart-hopping Access Point Controllers and Access Points

Upgrader Tool Guide

RTX

Firmware updates procedures:

AP Host

The AP Host software can be updated without overwriting the configuration, since the configuration is stored in the local folder on the AP Host, which is mapped to the docker containers.

To update the AP Host software:

1. Stop the OTAS Controller, VAP-Spawner and AP Host web page containers.
2. Kill all VAP containers.
3. Run the AP Host installation script.
4. Reboot

RTX3300 dongle

The RTX3300Dect software, which runs on the dongle, is packed as part of the VAP docker image, located in **/tmp/Rtx3300_492.fws**

The update process has not been integrated into the Philips Upgrader tool,

As of today, 2022/10/28, the way to initiate a firmware update is to send a unix signal to the ap-application inside a VAP, which will then start the firmware update on the dongle associated with the VAP.

This is done with

```
$ docker exec <container id> killall -USR2 app
```

Where <container id> is the VAP to use.

Having to know VAP container id's is not user friendly, and three others should be considered:

1) Make a list of compatible RTX3300Dect versions for the given VAP and let the VAP compare with the version returned from the dongle. Then start a firmware update if the version from the dongle is not supported. A problem with this approach is that the user does not control when the update process is started. Many dongles could start updating at the same time, which would cause downtime in the system.
2) Put a firmware update button on the VAP web page, which executes a script inside the container to send the unix signal to the ap-application, which will then start the update. It will be up to the user to compare firmware versions on the VAP web page and decide when to initiate an update.
3) React to a firmware update command from the Philips Upgrader tool and start firmware update. It should be verified that it is okay to just download a dummy firmware file to the VAP from the Upgrader. Another thing to investigate is whether the user is able to see the current RTX3300Dect version in the Upgrader.

AP-Relay

The AP-Relay software is updated through the Cisco DNA Center.

References

CIsco Systems, I. (n.d.). *Cisco Catalyst 9120 Access Point Deployment Guide.* Retrieved from www.cisco.com: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/guide-c07-742311.html

FCC Caution.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two c onditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: -Reorient or relocate the receiving antenna. -Increase the separation between the equipment and receiver. -Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. -Consult the dealer or an experienced radio/TV technician for help. The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.