



Sales & Partner Training
Worldwide Sales Strategy & Operations



Cisco Wireless Update

Carlo Terminiello, EMEAR Technical Marketing Engineer, Wireless Networking Group

PIW 31st May 2017



Agenda

01

Introducing WLC 3504

02

Access Point Update

03

8.4 / 8.5 Software Features

04

Mobility Express Update

DNA in Mobility Solutions

Reduce Cost & Complexity

- ❑ Public PnP with ME
- ❑ EoGRE tunnel Fallback
- ❑ Cisco Apple and ISE BPs

8.5

- Apple + Cisco
 - Optimize Wi-Fi Connectivity
 - Prioritize Business Apps
 - Integrate Collaboration



- Automation
 - Flexible Radio Assignment
 - WLAN Express Setup
 - Plug n Play Provisioning



- Visibility
 - Easy Monitoring & troubleshooting
 - App & Device Awareness
 - Service Assurance



Lower Risk

- ❑ Identity PSK
- ❑ Encrypted Tunnels

- ISE 2.2/TrustSec
 - BYOD Provisioning
 - 802.1x Authentication
 - Guest Access
- StealthWatch
 - Visibility and Segmentation
 - Threat Detection
 - BYOD Monitoring



- Open DNS
 - Category-Based Filtering
 - Policy Segmentation
 - Security Activity Monitor
- Protect the air
 - Interference and Air Quality
 - Detect Rogues and attacks



Faster Innovation

- ❑ WLC 3504
- ❑ vWLC on AWS
- ❑ APEX Modules

8.5

- Analytics
 - Presence Analytics
 - Location based Analytics
 - Verticalization
- User Engagement
 - Custom Guest Experience
 - Location Specific Portal
 - Connected Visitors Analytics
- Mobile Applications
 - Location based Engagement
 - 3rd party App integration
 - Programmability & extensibility



DNA Mobility Innovations Journey



- Flexible Radio Assignment
- Hyperlocation
- AP Plug n Play
- ATF – Client Fair-sharing
- Smart Licensing

- Cisco + Apple
- ATF on Mesh
- HTTP URL filtering
- CMX on Cloud
- Easy QoS + PnP
- Client Troubleshooting tool

- [TrustSec](#)
- [OpenDNS integration](#)
- [HTTPS URL Filtering](#)
- [Zero-touch Setup for vWLC](#)
- [ISE Best Practice defaults](#)
- [Hyper-V Support](#)

- ✓ [vWLC on AWS](#)
- ✓ [WLC 3504](#)
- ✓ [ME enhancements](#)
- ✓ [Identity PSK](#)
- ✓ [Encrypted Tunnels](#)
- ✓ [EoGRE tunnel Fallback](#)
- ✓ [U3 Interface for Ericsson](#)
- ✓ [Microsoft CNAME](#)
- ✓ [APeX](#)

8.2

8.3

8.4

8.5

DNA Mobility Innovations 8.5



- vWLC on AWS
- ME Enhancements



- Identity PSK
- Encrypted Tunnels
- EoGRE tunnel Fallback
- U3 Interface for Ericsson
- Microsoft CNAME



- WLC 3504
- APeX Program for Modules



Architecture

Security & Services

Hardware

Agenda

01 Introducing WLC 3504

02 Access Point Update

03 8.4 / 8.5 Software Features

04 Mobility Express Update

Wireless Controller Portfolio



Platforms &
Virtualization

Large Enterprise, Branch
Control at Central Site

Small Network

Mobility Express

50 APs/1000 Clients AP 18xx
100 AP/2000 Clients: AP2/3K
Flexconnect mode



1-100 APs

Mid-size Enterprise, Branch
Control at Central Site

Cisco vWLC

3000 APs
32000 Clients
Flexconnect mode



Cisco 3504

150 APs
3000 Clients
4 Gbps



Cisco 5520

1500 APs
20,000 Clients
20 Gbps



Cisco 8540

6000 APs
64,000 clients
40 Gbps



150-1500 APs

1500-6000 APs

WLC3504 Series Wireless LAN Controller

Industry's first Wireless LAN Controller with Multigigabit Ethernet

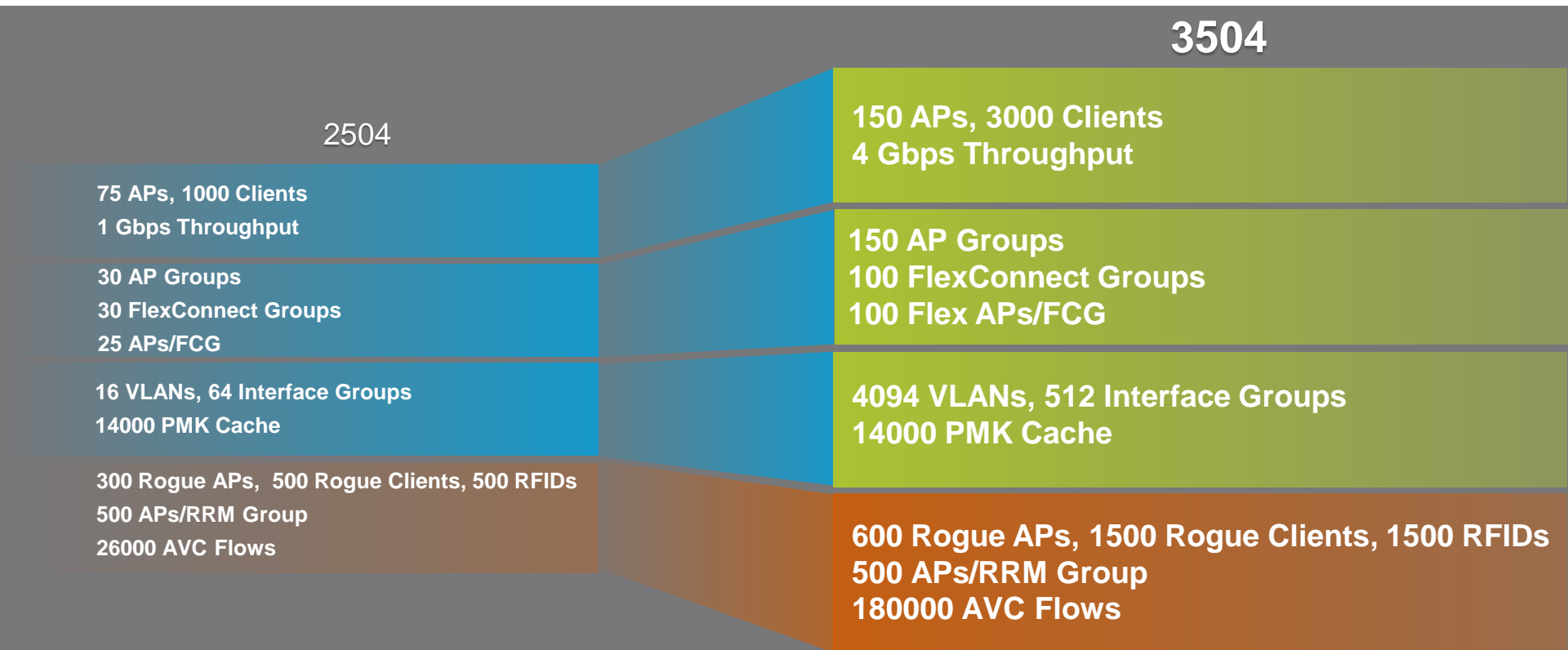


Access Points	150 in Centralized mode
Clients	3000 in Centralized mode
Throughput	4Gbps
HA Support	Dedicated RP for HA SSO
Service Support	Dedicated SP
Form factor	Side by Side Primary/HA rack mount (1 RU)
I/O interface	mGig + 4x1GE, USB
Console:	RJ45, mini USB

Access Points	<ul style="list-style-type: none"> ✓ Powerful enough to handle 802.11ac Wave 2 traffic loads ✓ Up to 150 AP, 3000 clients, 4Gbps
Seamless Scalability	<ul style="list-style-type: none"> ✓ Seamless migration (configuration migration tool from 2504 and 5508) ✓ Seamless WLC portfolio – feature parity across 3504 and 5520
Flexible Deployment	<ul style="list-style-type: none"> ✓ mGig or 4x1GE ✓ Rack Mount, Cabinet, Desktop ready: <ul style="list-style-type: none"> • 1RU, side by side Rack Mount • Quiet fanless for cabinet, desktop (up to 30C ambient) ✓ 10" depth to fit nicely in cabinet
HA Support	<ul style="list-style-type: none"> ✓ Pairing with stateful switchover

Compact (1 RU) | mGig ready | Dedicated RP/SP ports | HA SSO | Side by Side rack mount

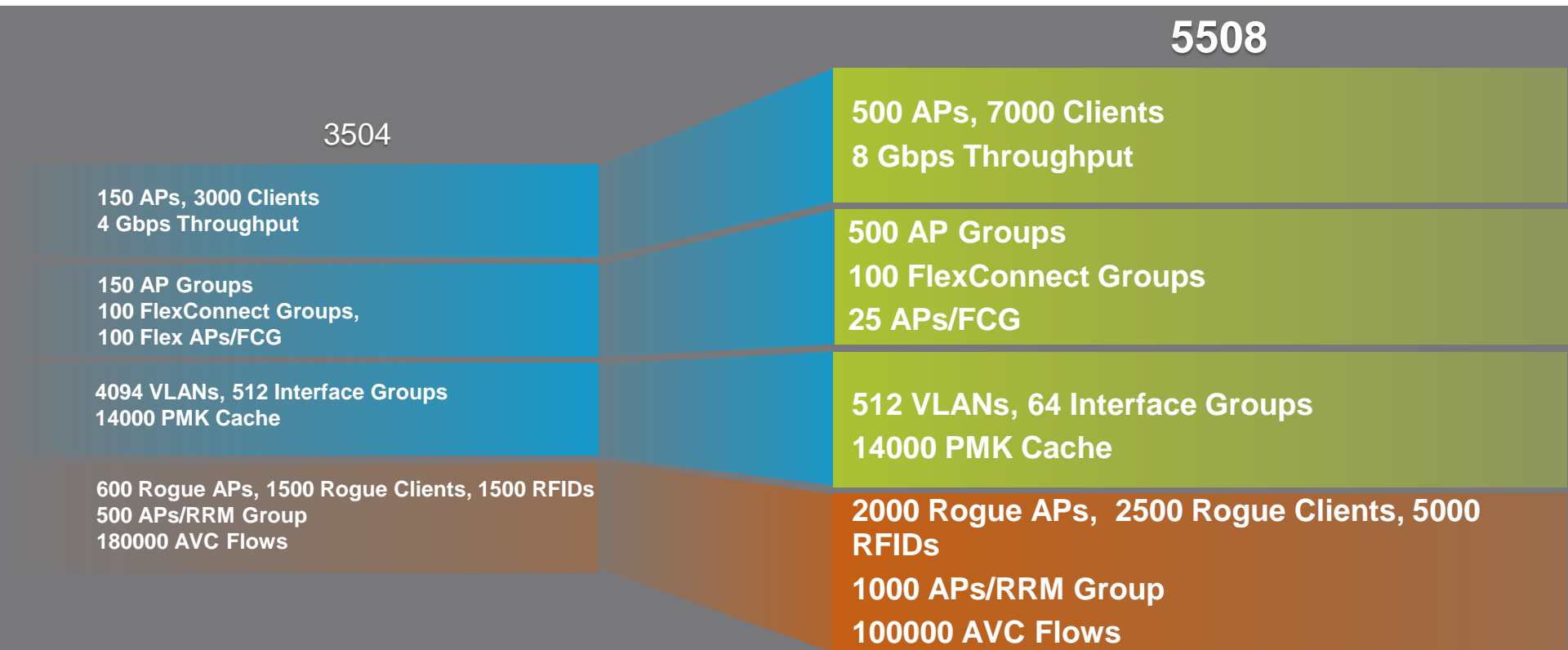
Evolution of Wireless LAN Controllers



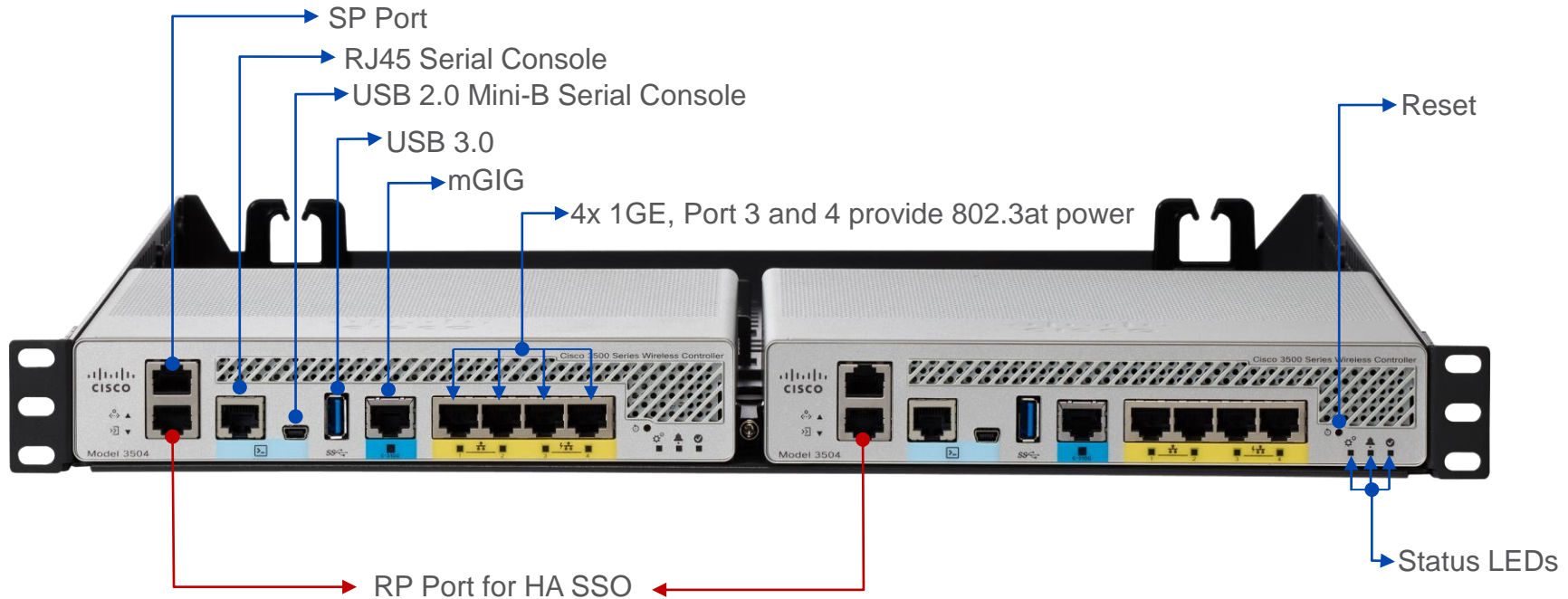
Evolution of Wireless LAN Controllers



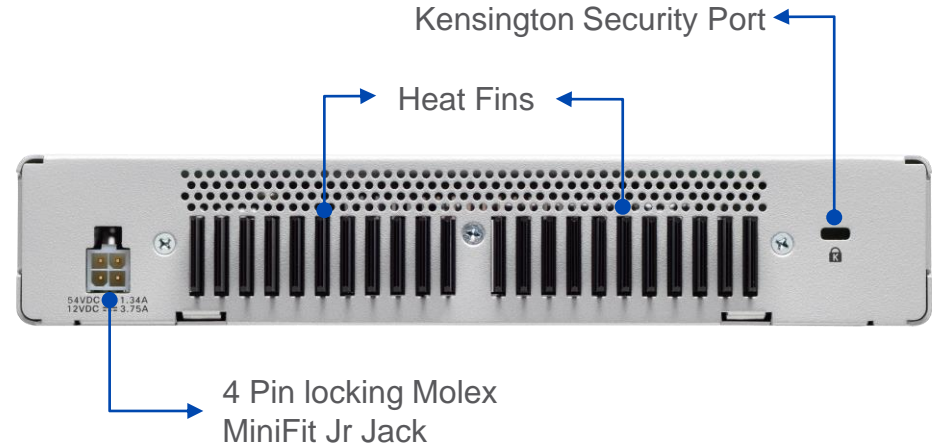
For Your
Reference



WLC 3504 Interfaces - Front



WLC 3504 Interfaces - Back



Smart Fan. Fan OFF for $< 30^{\circ}\text{C}$ and runs when temperature $> 30^{\circ}\text{C}$ ambient

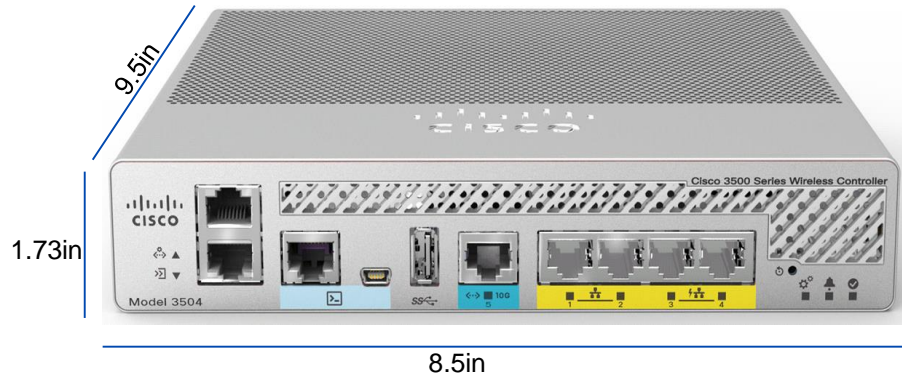
WLC 3504 Power Supply

- Single Power Supply
- PWR-115W-AC : WLC 3504 uses a new dual 12V/54VDC output power supply (with sufficient capacity to support two 802.3at PoE out ports and 12VDC capacity for the system.
- WLC 2504 Power Supply is not compatible with WLC3504.



WLC 3504 Dimensions & Environmental

- Dimensions:
 - 8.5 (W) x 9.5 (D) x 1.73 (H) in
 - 215.9 (W) x 341.3 (D) x 43.94 (H) mm
- Width to allow side-by-side installation in single 1RU 19" rack slot



WLC 3504 shall have the following environmental specifications:

- Non-operating (storage) temperature: -20 to 70C
- Operating temperature: 0 to 40C
- Operating humidity: 5 to 95% (non-condensing)
- Storage Humidity: 0% to 95% RH non-condensing
- Heat dissipation(without PoE): 47W, 160BTU/hr
- Heat dissipation(with PoE): 98W, 335BTU/hr

WLC3504 Series Wireless LAN Controller

Small Form factor, Fast, Flexible, Resilient and **DNA Ready**



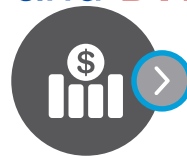
High Scalability

- Powerful enough to handle 802.11ac Wave 2 traffic loads
- Flexible connectivity (1- 2.5 - 5 Gbps ports)
- 4-Gbps throughput
- Up to 150APs and 3000 clients
- Seamless migration (USB + configuration migration tool from 2504 and 5508)



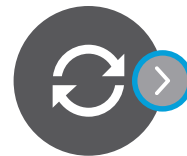
Integrated Services

- Apple FastLane support
- TrustSec & OpenDNS support
- Identity PSK
- Application visibility and control
- Policy classification
- Guest/BYOD services
- Bonjour/Chromecast gateway



Return on Investment

- Seamless WLC portfolio – feature parity across 3504, 5520 and 8540
- Simplified licensing (RTU)
- License portability (3504, 5520 and 8540)
- Simplified deployment
- Scale as needed (add one AP at a time)
- 1- 2.5 - 5 - upgrade as you grow & future proof your investments



High Availability and Resiliency

- Pairing with stateful switchover
- Fast restart - enhanced uptime
- Quiet fanless for cabinet, desktop environments (up to 30C ambient)
- Easy maintenance

WLC 3504 Features

- **Multiple Setup Options**
 - Auto-Install, CLI Setup Wizard, Over-the-air-provisioning etc.
- **Support of all AP modes of operation (Local, FlexConnect, Monitor, Rogue Detector, Sniffer, Bridge, and Flex+bridge)**
- **AP Platform Support**
 - 1600, 2600, 3500, 3600
 - 1700, 2700, 3700
 - 1800, 2800, 3800
 - 1815T, OEAP 1810, OEAP 600,
 - 1815W, 1810W, 702I, 702W
 - 1530, 1552WU, 1550, 1560, 1570

Software Features

- Internal DHCP Server
- Data DTLS
- Multicast Support
 - Multicast-Multicast
 - Multicast-Unicast
- Netflow
- mDNS
- Software Update via USB

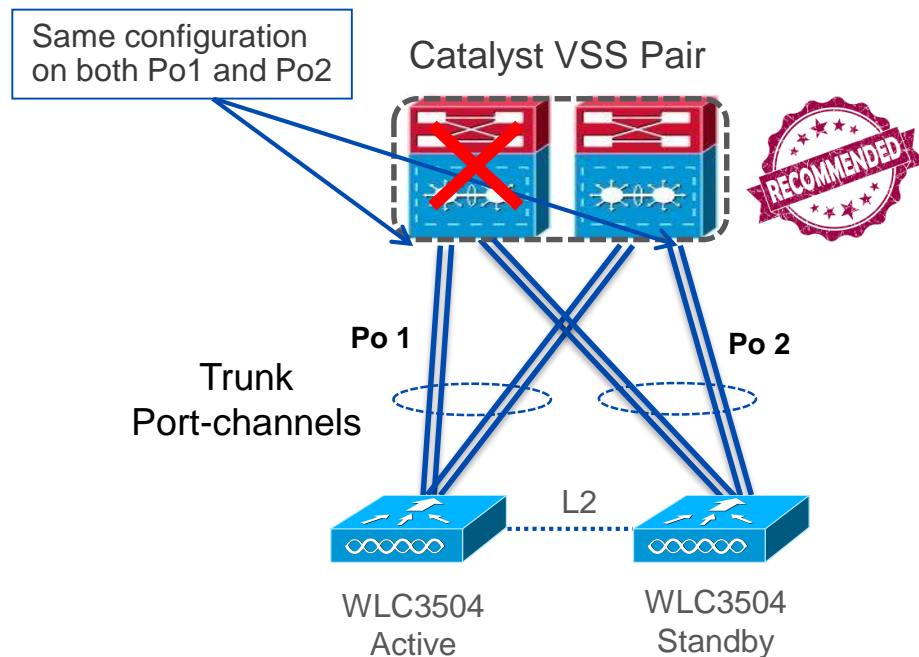
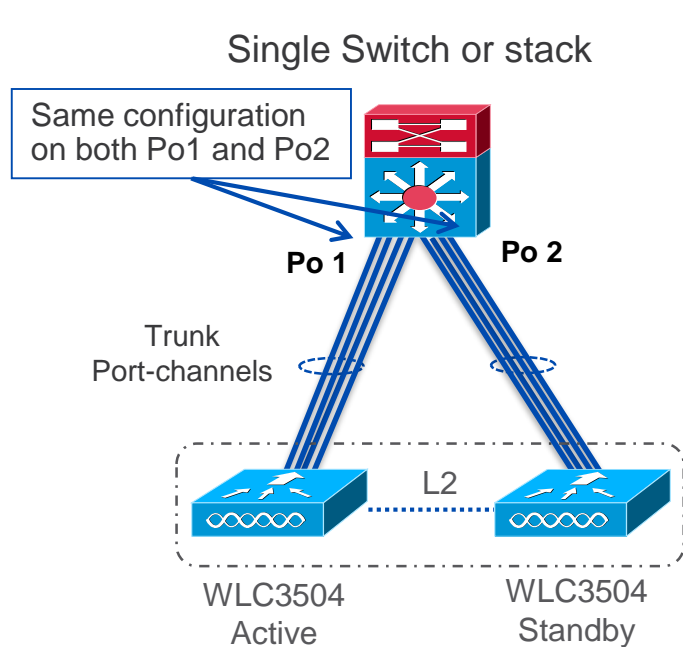
High Availability - SSO



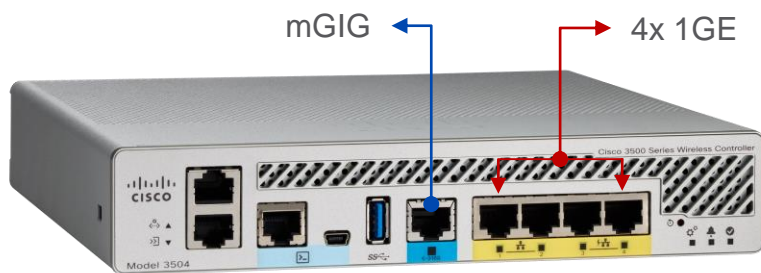
- True Box to Box High Availability i.e. 1:1
 - One WLC in Active state and second WLC in Hot Standby state
 - Standby unit continuously monitors the health of Active WLC via dedicated link
- Downtime during failover is greatly reduced:
 - **2 - 100 msec** for a box failover (Active WLC crashes, system hangs, manual reset or forced switch-over)
 - **350-500 msec** in the case of power failure on the Active WLC
 - **Few seconds** in the case of network failover (gateway not reachable)
- Configuration on Active is synched to Standby WLC
 - This happens at startup and incrementally at each configuration change on the Active
 - What is synced - Access Point data base, Client in "RUN" state, Sleeping Client data base, OEAP clients, Internal DHCP, Static CAP config and stats
- There is no preemption in Controller SSO
 - When the failed Active WLC comes back online it will join as Hot Standby

High Availability – Design and Deployment

Connecting WLC3504 HA Pair to the wired network

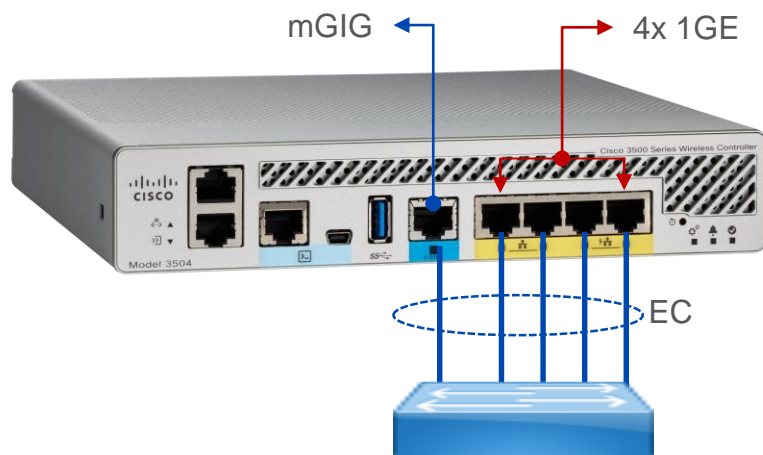


Data Ports Behavior



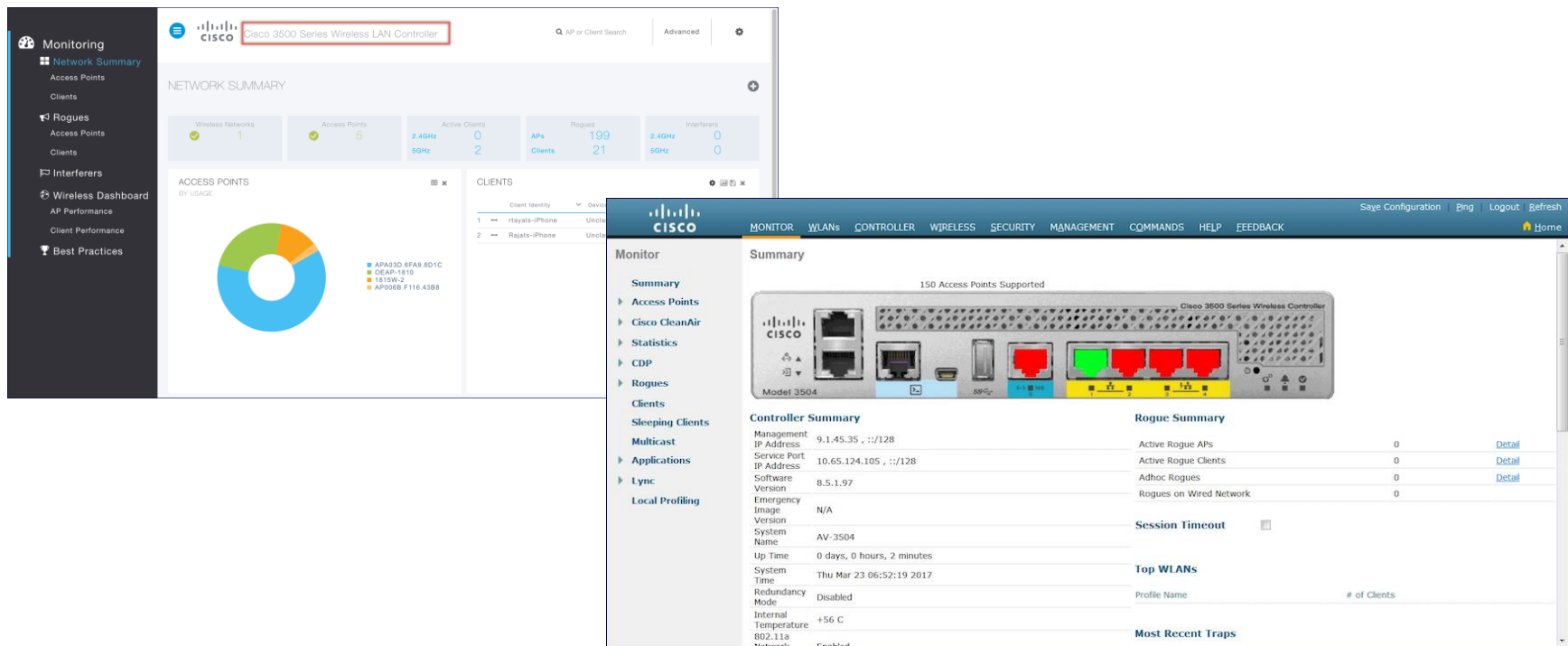
- mGig and 4xGE ports can be used for switch connectivity
- Only 4xGE ports can be used for direct AP connectivity
- mGig port can negotiate 1G, 2.5G, and 5G
- If mGig is enabled for 5G, 4xGE ports will be set to 100 Mbps
- If mGig is enabled for 2.5G, GE1 & GE2 will stay at 1G and GE3 & GE4 will be set to 100 Mbps

Data Port behavior and LAG Support



- 4xGE can be used for link aggregation
- If mGig is set to 1G, it can participate in LAG with GE ports
- LACP and PAgP are not supported on the controller
- No direct AP support on mGig and therefore can not connect AP to mGig

WLC 3504 Management WebUI



Software Update

- Supported methods are
 - TFTP, FTP, SFTP, HTTP and now **USB**
- Hookup the USB with single FAT partition containing the image
- Follow the same method as that of FTP/TFTP image download with mode being “USB”

The screenshot shows the Cisco Controller's web interface for downloading a file to the controller. The 'Commands' tab is selected. On the left, a sidebar lists various commands like 'Download File', 'Upload File', 'Reboot', etc. The main area is titled 'Download file to Controller'. It has a 'File Type' dropdown set to 'Code'. Below it, the 'Transfer Mode' is set to 'USB' (highlighted with a red box). Under the 'Server Details' section, the 'USB Path' is '/' and the 'USB Filename' is 'AS_3500_8_5_1_94.aes' (both highlighted with red boxes). At the top right of the main area, there are 'Clear' and 'Download' buttons, with the 'Download' button highlighted with a red box.

(Cisco Controller) >transfer download mode usb

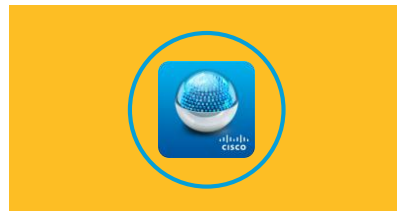
WLC 3504 Interoperability



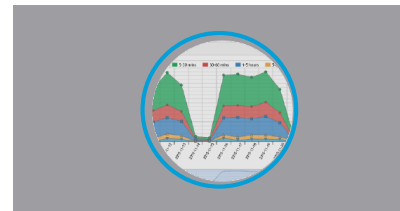
AireOS 8.5



ISE 2.2

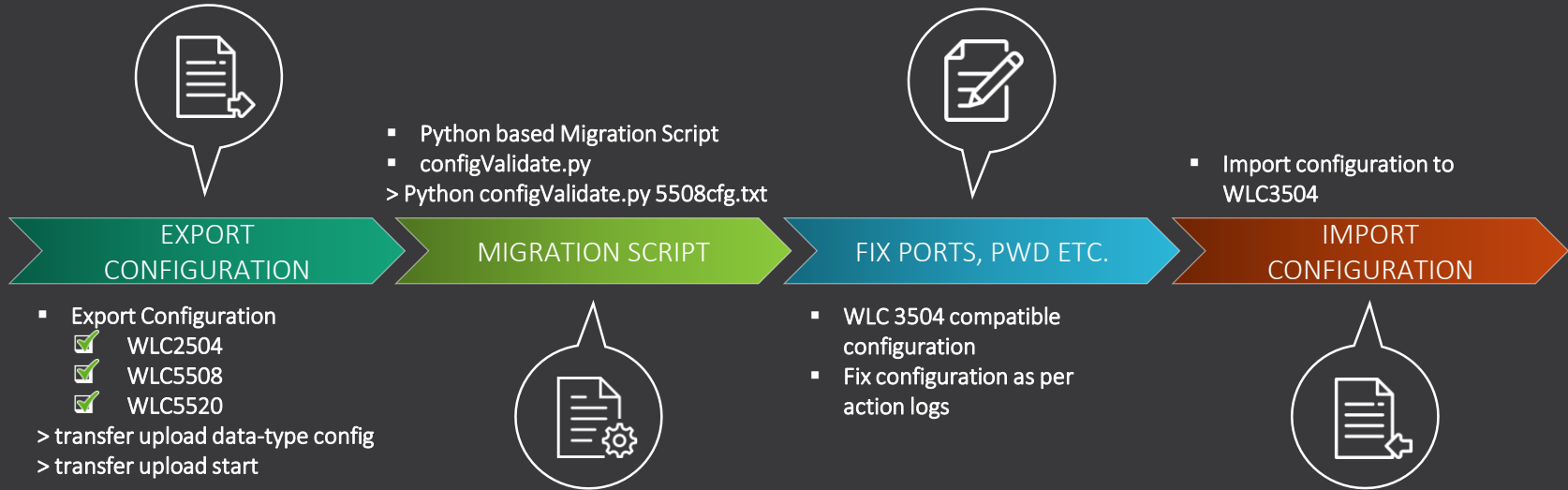


PI 3.2

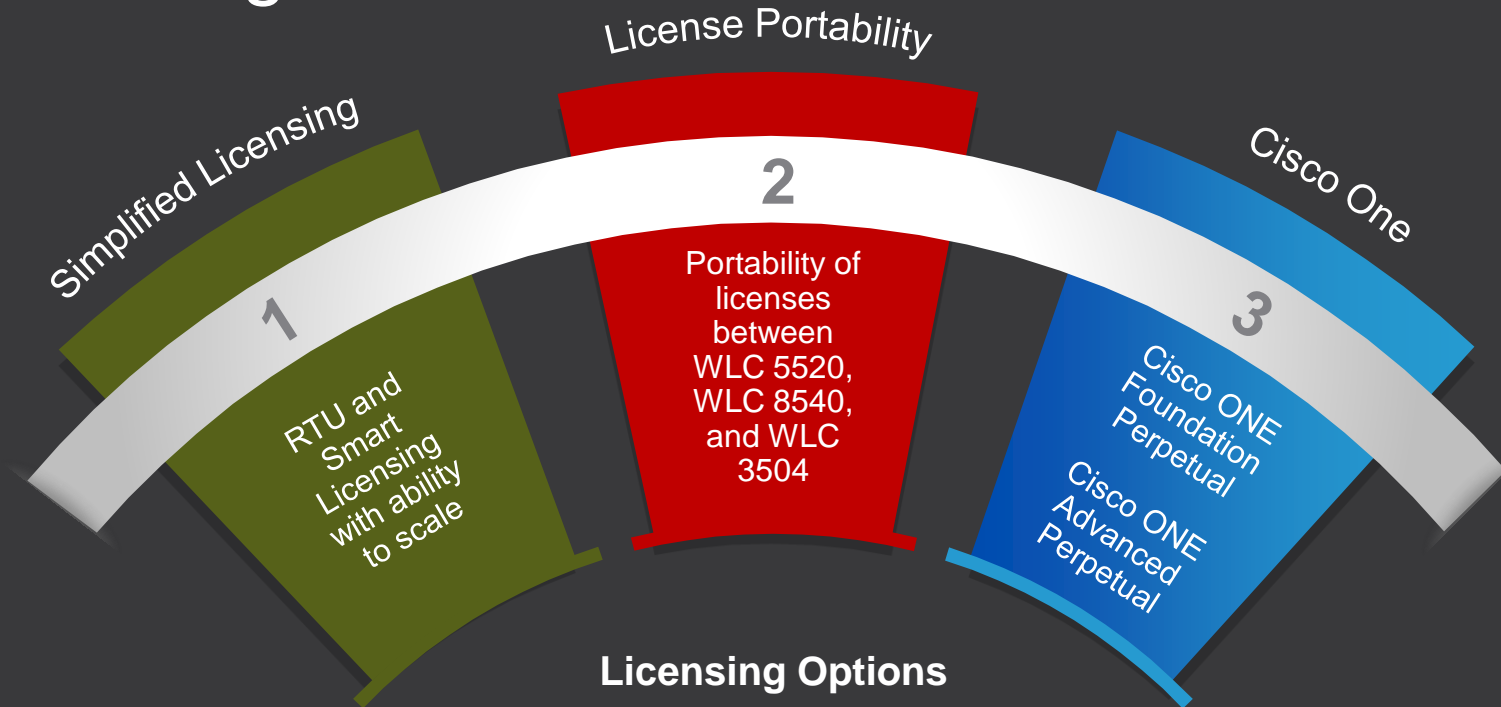


**CMX10.x
MSE 8.x**

Migration



Licensing



Agenda

01

Introducing WLC 3504

02

Access Point Update

03

8.4 / 8.5 Software Features

04

Mobility Express Update

Access Point - Update

- AP-1815 - Indoor AP
- AP-1540 - Outdoor AP
- APeX AP- 3800 Module Program

Access Point Software... Quick History

- **SoS** – Stuart Operating System CY1993 – Pre-802.11 & 340 Series
 - **Aironet OS** (based on VxWorks Wind River) CY1998
 - Note: Cisco Acquires Aironet CY2000 – with intent to move to IOS
- **aIOS** – Autonomous IOS (Stand-alone) CY2001
- **Unified IOS** (controller based) CY2005
- **AP-COS** – *NEW* **(LINUX BASED)**

The following Access Points now support Cisco AP-COS



Cisco Aironet 802.11ac Wave 2 Access Point Portfolio

Industry's most comprehensive and innovative

Enterprise Class

Mission Critical

Best in Class

DNA Ready | RF Excellence | CMX | Centralized, FlexConnect or Mobility Express

Dual 5 GHz | Flexible Radio | HDX

Future Proof



1815

Indoor / High-powered Indoor Wall Plate / Teleworker

- 2x2:2SS 80 MHz
- 867 Mbps Performance
- Tx Beam Forming
- Integrated BLE Gateway¹
- Max Transmit Power (dBm) per local regulations²
- 3 GE Local Ports, including 1 PoE out³
- Local ports 802.1x ready³
- USB 2.0⁴



1830

- 3x3:2SS 80 MHz
- 867 Mbps Performance
- Tx Beam Forming
- 1 GE Port Uplink
- USB 2.0



1850

- 4x4:3SS 80 MHz
- 1.7 Gbps Performance
- Internal or External Antenna
- Tx Beam Forming
- 2 GE Ports Uplink
- USB 2.0



2800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink
- CleanAir and ClientLink
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0



3800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink or 1 GE + 1 mGig (5G)
- CleanAir and ClientLink
- StadiumVision
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0
- Investment Proof Modularity

Cisco Aironet 802.11ac Outdoor Access Point Portfolio

Industry's most comprehensive and innovative portfolio

DNA Ready | RF Excellence | CMX

New*



1540

- 802.11ac Wave 2, MU-MIMO
- 2x2:2, 80MHz, 867 Mbps
- Ultra low profile
- Internal antenna model (I)
- Internal directional antenna model (D)
- PoE (802.3af) power
- Centralized, FlexConnect, Mesh* and Mobility Express

New



1560

- 802.11ac Wave 2, MU-MIMO
- 3x3:3, 80MHz, 1.3Gbps (I)
- 2x2:2, 80MHz, 867Mbps (E/D)
- Internal or External antenna model (I/E)
- Internal directional antenna model (D)
- SFP
- Flexible Antenna Ports
- CleanAir and ClientLink
- Centralized, FlexConnect, Mesh and Mobility Express



1570

- 802.11ac Wave 1
- 4x4:3 80 MHz; 1.3 Gbps
- External antenna model (EAC)
- Cable Modem model (IC/EC)
- SFP
- GPS
- PoE Out 802.3at (Ext Ant. only)
- Flexible Antenna Ports
- CleanAir and ClientLink
- Modularity (Ext Ant. only)
- Centralized, FlexConnect and Mesh
- Cable Modem Version Only (IC/EC)
- DOCSIS 3.0, 24x8
- Internal or External antenna

802.11ac Wave 2

Where the 1815 fits in the Aironet 802.11ac Wave 2 Portfolio

Industry's most comprehensive and innovative AP portfolio

Enterprise Class

Mission Critical

Best in Class

DNA Ready | RF Excellence | CMX | Centralized, FlexConnect or Mobility Express

Dual 5 GHz | Flexible Radio | HDX

Future Proof

Beginning CY17



1815

Indoor / High-powered Indoor Wall Plate / Teleworker

- 2x2:2SS 80 MHz
- 867 Mbps Performance
- Tx Beam Forming
- Integrated BLE Gateway¹
- Max Transmit Power (dBm) per local regulations²
- 3 GE Local Ports, including 1 PoE out³
- Local ports 802.1x ready³
- USB 2.0⁴



1830

- 3x3:2SS 80MHz
- 867 Mbps Performance
- Tx Beam Forming
- 1 GE Port Uplink
- USB 2.0



1850

- 4x4:3SS 80MHz
- 1.7 Gbps Performance
- Internal or External Antenna
- Tx Beam Forming
- 2 GE Ports Uplink
- USB 2.0



2800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink
- CleanAir and ClientLink
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0



3800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink or 1 GE + 1 mGig (5G)
- CleanAir and ClientLink
- StadiumVision
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0
- Investment Proof Modularity

Aironet® 1815 Series 802.11ac Wave 2 Indoor Access Points



Cisco Aironet® 1815 Series

The Cisco Aironet 1815 Series Access Points (APs) are

- Comprised of four separate low-cost, sleek APs
- Ideal for organizations looking to address growth but have budget restrictions
- Minimizing total cost of ownership while delivering advanced features like 802.11ac Wave 2
- Easy to deploy and manage with Cisco Mobility Express

Ideal for Small to Medium sized Deployments

Which Access Point is Right for You?

\$495



- 1815i is the ideal access point for small to medium-sized businesses looking for cutting-edge, enterprise-level function and features. With its sleek form factor, the 1815i is a discrete and powerful wireless solution available at an affordable price.

\$595



- 1815t is targeted for teleworkers and micro-branch deployments of all industries so no longer will geography get in the way of work place productivity

\$495*



*including
WLC
license

- 1815w is wall plated mounted access point that is perfect for hospitality, residential halls or other multi-dwelling unit deployments

\$595



- 1815m has more transmit power to cover a larger area and is the perfect AP for budget-conscious organizations that need a wide coverage zone.

Ordering Information

PID	Description	List Price
AIR-AP1815i-x-K9 / K9C	Infra .11ac wave 2	\$495
AIR-AP1815m-x-K9 / K9C	Infra .11ac wave 2 – high power	\$595
AIR-AP1815w-x-K9 / K9C	Wall Plate .11ac wave 2	\$495 + WLC license included
AIR-AP1815t-x-K9	Teleworker .11ac wave 2	\$595
AIR-AP-BRACKET-8	Infra mounting bracket	\$23
AIR-AP1815W-KIT	Wall Plate spacer for cable pulling	\$34
AIR-AP-BRACKET-W3	Wall Plate mounting bracket	\$25

* -K9C = Mobility Express enabled

Aironet® 1815 Series Promotion

Any 1815 Series AP configured with Mobility Express qualifies for 1 Year of CMX Cloud at no additional cost!



With Cisco® Mobility Express and Cisco Connected Mobile Experiences (CMX) Cloud, you can:



Deploy simple, fast, low-cost wireless network and location services in minutes



Provide enterprise-class Wi-Fi features, professional captive guest portals, and presence analytics without appliance and management overhead



Monitor and troubleshoot the network via the Cisco Wireless Mobile App, available in the Google Play Store and Apple App Store

Cisco Aironet® 1815I Series (Infrastructure)

Aironet® 1815I Series – Infrastructure

List Price \$495



Cisco Aironet® 1815i

- **Target Deployments** : Ideal for SMB deployments
- **Enterprise-class** : Dual Radio, Dual Band, 80MHz, 2x2 MU-MIMO, 802.11ac Wave 2 Access Point
- **Ethernet Ports** : 1x PoE uplink GigE port
- **PoE Support** : Can be powered with 802.3af or 802.at power
- **Small Form Factor** : Sleek design with integrated antennas for optimal wireless coverage in a small form factor 6in x 6in x 1.2in
- **Mobility Express Support** : Supports 50 APs and 1000 clients in a Mobility Express deployment
- **Integrated Bluetooth Low Energy radio**

Cisco Aironet[®] 1815M Series (High Power)

Aironet® 1815M Series – High Power

List Price \$595

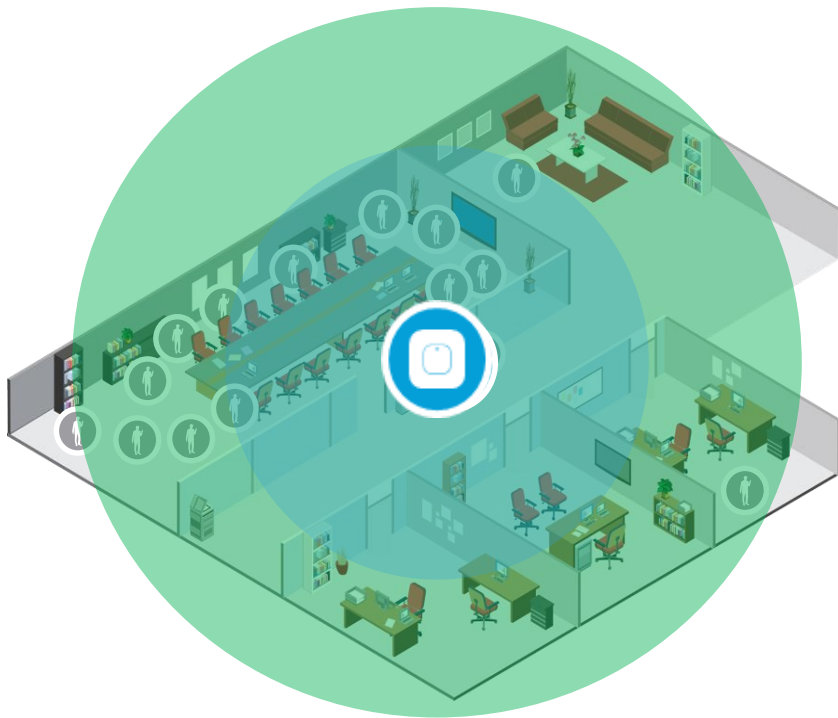


Cisco Aironet® 1815m

- **Target Deployments** : Ideal for SMB deployments in emerging markets with emphasis on coverage
- **Enterprise-class** : Dual Radio, Dual Band, 80MHz, 2x2 MU-MIMO, 802.11ac Wave 2 Access Point
- **Ethernet Ports** : 1x PoE uplink GigE port
- **PoE Support** : Can be powered with 802.3af or 802.at power
- **Small Form Factor** : Sleek design with integrated antennas for optimal wireless coverage in a small form factor 6in x 6in x 1.2in
- **Mobility Express Support** : Supports 50 APs and 1000 clients in a Mobility Express deployment
- **+4dB Tx Power per chain compared to 1815i**
- **Integrated Bluetooth Low Energy radio**

* Q2'CY'17 demo
Q3'CY17 target availability

Aironet® 1815I vs 1815M coverage



● Capacity - 1815I

● Coverage - 1815M

Cisco Aironet® 1815W Series (Wall Plate)

Aironet® 1815W Series – Wall Plate

List Price \$495, License Included



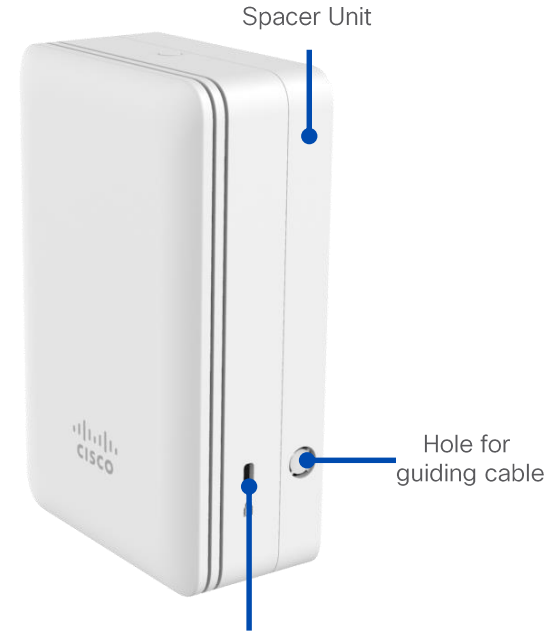
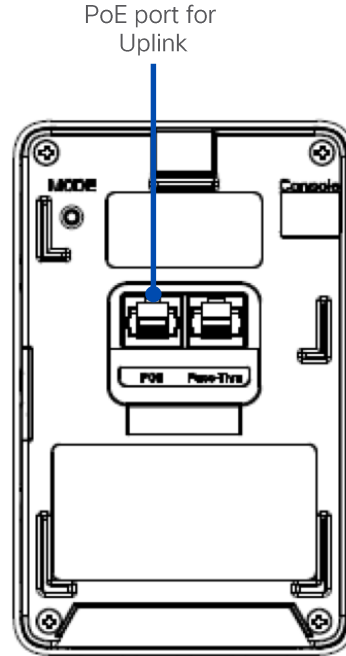
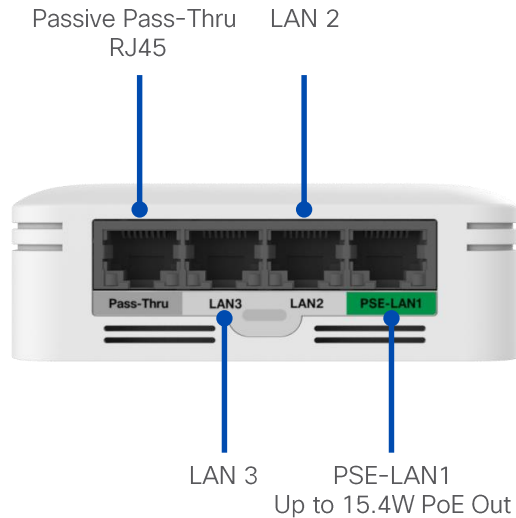
Cisco Aironet® 1815w

- **Target Deployments** : Higher Education and Hospitality deployments, providing wired and wireless access
- **Enterprise-class** : Dual Radio, Dual Band, 80MHz, 2x2 MU-MIMO, 802.11ac Wave 2 Access Point
- **Ethernet Ports** : 3x GigE Wired Ethernet ports + 1x uplink GigE port + 1x passive pass-through RJ45. Up to 3x GigE Wired Ethernet ports can be locally switched or tunneled back to Wireless LAN Controller
- **PoE Support** : Can be powered with 802.3af or 802.at power. 803.af PoE out on PSE-LAN 1 port when powered with local DC power using either AIR-PWR-C or AIR-PWR-D
- **Small Form Factor** : Sleek design for ease of mounting to numerous global wall junction standards or with a spacer kit directly on the wall.
- **Mobility Express Support** : Supports 50 APs and 1000 clients in a Mobility Express deployment

Aironet® 1815W – Features

- ❑ **AP Mode**
 - Local, FlexConnect, and Sniffer Mode. Can also be configured to operate as Office Extend
- ❑ **DTLS**
 - Control DTLS for WLAN and RLAN
 - Data DTLS for WLAN and RLAN. Disabled by default.
- ❑ **Multi-Client support on Wired LAN ports**
 - Up to of 4 clients supported on each Wired LAN port
- ❑ **Authentication and Security**
 - Advanced Encryption Standard (AES) for Wi-Fi Protected Access 2 (WPA2)
 - 802.1X, RADIUS authentication, authorization and accounting (AAA) on WLAN and RLAN
- ❑ **CDP and LLDP on PoE Uplink and LAN1 (PSE)**
 - On PoE Uplink, CDP runs first to negotiate power with switch. If it fails, then LLDP runs to negotiate power
 - On LAN 1(PSE) port, CDP is not supported. LLDP support on LAN1(PSE) and is fixed power on LAN1 PSE port (not negotiable)
- ❑ **MAC filtering**
- ❑ **Dynamic VLAN assignment**
- ❑ **FlexConnect Local switching on RLAN**
- ❑ **Web-Auth support**
- ❑ **Cisco Mobility Express supported on AIR-AP1815W**

Aironet® 1815W – Interfaces



Configuring Aironet® 1815W

Wireless and Wired Access

AIR-AP1815W Access Point is designed keeping Higher-Ed and Hospitality customers in mind. They are an ideal fit for University dorm rooms and Hotel Guest rooms to provide simultaneous Wireless and Wired access. In University dorm rooms, Ethernet devices can be used to connect IP Phones, entertainment devices like Xbox etc. In Hospitality (Guest Rooms), it can be used for providing connectivity to Set-top devices, IPTV, IP Phone, as well as Wired internet connectedly to guests.

AIR-AP1815W has three LAN ports to offer Ethernet services for wired devices in the rooms. These services are via Remote LANs on the controller. Remote LAN are for Wired clients like WLANs are for Wireless clients.

AIR-AP1815W supports two deployment modes for the client wireless and wired data traffic. Local Mode (client data traffic delivered to the controller over a CAPWAP tunnel) or FlexConnect mode where client data traffic is dropped locally or tunneled back to the controller over the CAPWAP tunnel.

Cisco Aironet® 1815T Series (Teleworker)

Aironet® 1815T Series – Office Extend

List Price \$595



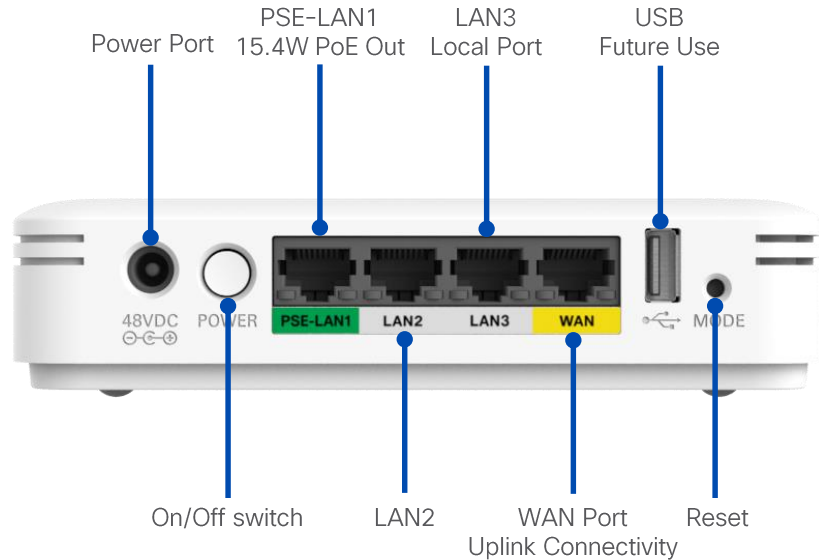
Cisco Aironet® 1815T Series

- **Target Deployments** : Teleworker or Micro-branch deployments, providing **wired and wireless corporate access** to remote workers
- **Enterprise-class** : Dual Band with 802.11ac Wave 2, 80MHz, 2x2 MU-MIMO, 802.11ac Wave 2 Access Point
- **3 x GigE Ethernet Ports** : 1 x uplink GigE port, Up to 2 ports can be tunneled back to Wireless LAN Controller
- **Full PoE out** : 803.af on PSE-LAN 1 port. Powered with local DC power using either AIR-PWR-C or AIR-PWR-D
- **Small Form Factor** : Elegant design with integrated antennas for optimal wireless coverage and convenient cable management.

Aironet® 1815T – Features

- ❑ **AP Mode**
 - Office Extend
- ❑ **DTLS**
 - Control DTLS for WLAN and RLAN
 - Data DTLS for WLAN and RLAN
- ❑ **Multi-Client support on Wired LAN ports**
 - Up to of 4 clients supported on each Wired LAN port
- ❑ **Authentication and Security**
 - Advanced Encryption Standard (AES) for Wi-Fi Protected Access 2 (WPA2)
 - 802.1X, RADIUS authentication, authorization and accounting (AAA) on WLAN and RLAN
- ❑ **Personal SSID**
 - Support to configure and broadcast Personal SSID on 2.4 and 5 GHz for local networking

Aironet[®] 1815T – Interfaces



Deploying AIR-AP1815T

01 Manual Priming

Manually Prime the AIR-AP1815T Access Point with the IP address of the corporate controller IP address.

02 APIC-EM Private Cloud

Use Network PnP service in APIC-EM which resides in customer premises to provision the AIR-AP1815T Access Points. Access Point can download the AP configuration file from Network Plug and Play service which contains the controller information, AP Group, AP Name etc. and join the corporate controller.

03 APIC-EM Cisco Cloud Redirect

Use Cisco Cloud redirect service to redirect AIR-AP1815T Access Points to APIC-EM residing in customer premises. Access Point can then download the AP configuration file from Network Plug and Play service which contains the controller information, AP Group, etc. and join the corporate controller.

Aironet® 1815T – Configuring Personal SSID



CONNECT

Using any laptop, connect to LAN3 port on the 1815T. From a web browser, login to the OEAP UI via <http://10.0.0.1> using admin/admin as the default credentials.



CONFIGURE

Configure the Personal SSID on 1815T for local networking. On the OEAP UI, navigate to Configuration > SSID. Click on either 2.4 or 5 GHz radio and configure the personal SSID with security as WPA2-PSK or WPA-PSK.



ACCESS

Connect to Personal SSID to access the local network.

References

Cisco 1815 Series Web Page – <http://www.cisco.com/c/en/us/support/wireless/aironet-1815-series-access-points/tsd-products-support-series-home.html>

Cisco 1815I Data Sheet – <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738243.html>

Cisco 1815M Data Sheet – <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738499.html>

Cisco 1815W Data Sheet – <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738481.html>

Cisco 1815T Data Sheet – <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738482.html>

Cisco 1815W Deployment Guide – [http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b AP 1815 wall plate deployment guide.html](http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_AP_1815_wall_plate_deployment_guide.html)

New – AP-1540 Series Outdoor Access Points

Compact Outdoor Access Point

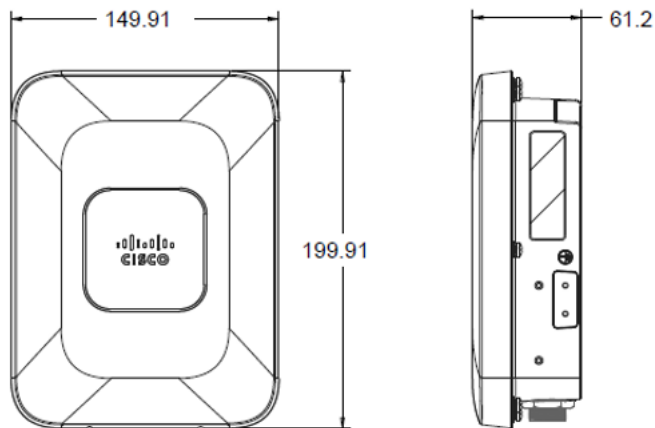


Cisco Aironet® 1540 Series

- Dual Radio 802.11ac Wave 2
- 2x2:2, 20/40/80 MHz channels
- Std. 802.3af power (13W)
- Small, lightweight (1.25kg)
- Ruggedized for Outdoor: IP65,
Temp -40 to +65° C

Exceptional Performance at Exceptional Price

AP1540 Joins Outdoor Line as “Little Brother”



Outer dimensions,
mm



[illegible]

Outdoor/Mesh SW Roadmap*

Not
committed yet

8.4 (Mar '17)

- Mesh support for AP1560
- Airtime Fairness (ATF) for Mesh deployments (1530/1570)
- Support for AP1540
 - Local
 - Flex
 - Mobility Express
 - MR1 – June 17

8.5 (Jul '17)

- Mesh support for AP1540

8.x (1H'18)

- WGB on Wave 2 APs
- Mesh for indoor Wave 2
- PtP for AP1560 & AP1540
- Daisy chain w/ 1560/1540

- Planned Releases; dates and content subject to change

3rd Party AP modules APeX Access Point eXtensions

A development program to enable an ecosystem of expansion modules for Cisco Wireless Access Points

Being introduced for the AP-3800i/e/p Series

3rd Party Module Ecosystem for 3802I/E/P

- The goal is to promote 3800 module development for IoT etc. enabling
 - ✓ Strategic Partners
 - ✓ 3rd Party solution vendors
- Permit AP-3800 to easily interface with custom hardware and popular developer hardware devices such as Raspberry Pi, Beagle-Bone, Intel Joule etc.
- To provide a development platform with HDK/SDK/APIs to enable IOT-Mobility convergence & design for both Hardware and Software based solutions
- Provide a module interface specification and design guidelines defining electrical, mechanical, thermal and RF characteristics.
- Almost anything can be developed, beacons, gateways, voice, security etc.

Module Development

Enable rapid prototyping with one of the popular development boards

1

Onboard

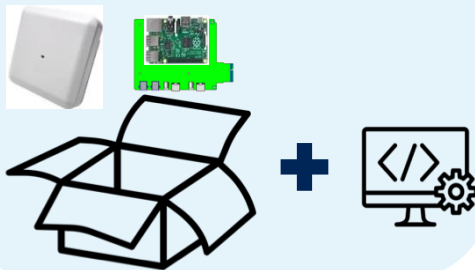
Developer onboarding via
DevNet



2

Develop

Module Development Kit
HDK | SDK



3

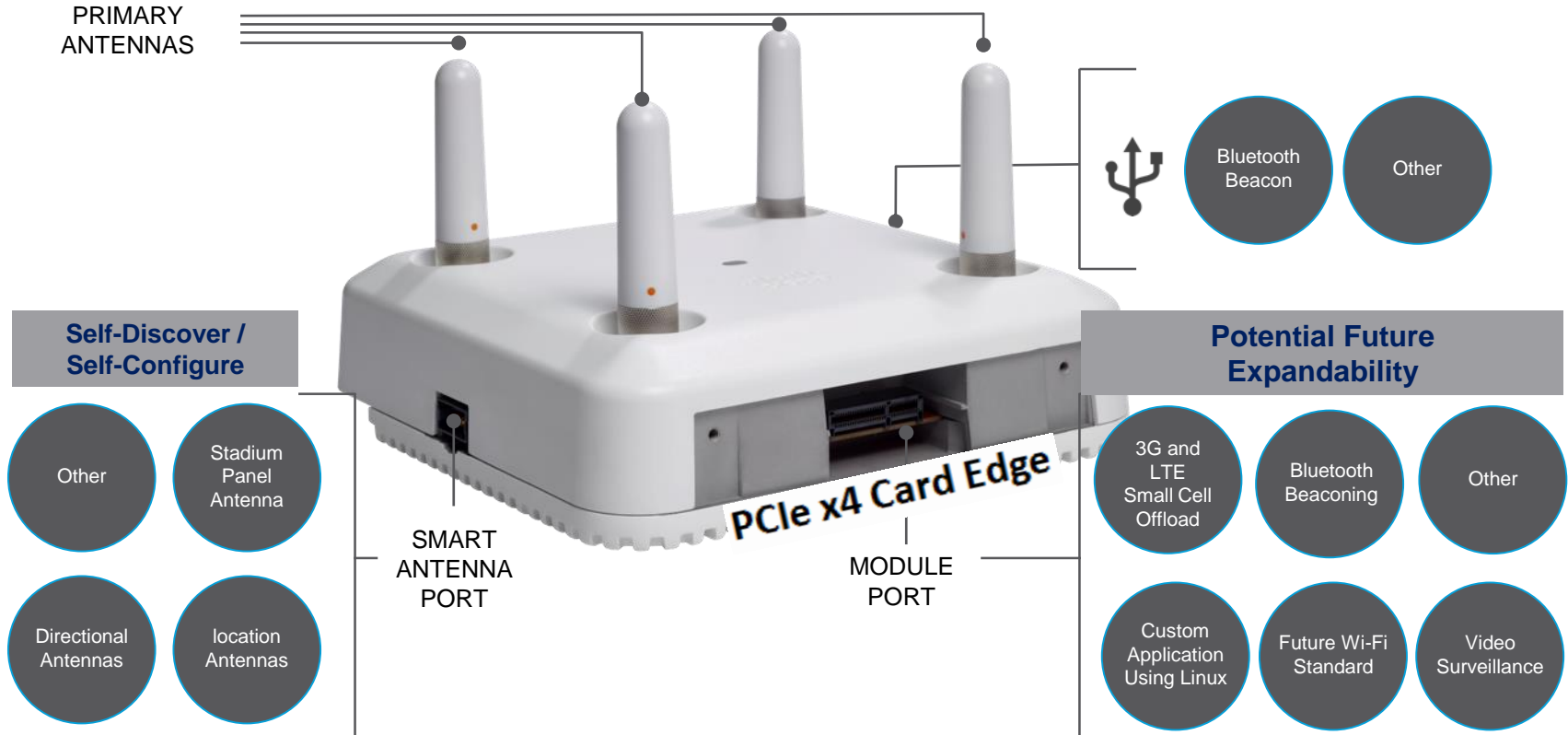
Productize

Developer productizes
module



Review of AP-3800i/e Port Functionality

Expandability and Investment Protection



AP-3800 Hardware Developer Kit



Prototype Carrier Board

Mounting accommodations

- 37xx/36xx EM module
- Raspberry Pi 1/2/3
- Beagle Bone Black
- Intel NUC
- Microcenter E100 Intel Gateway

Initial modules likely to be:

PoE adapter, Electronic Shelf Labeling, Physical Security / Camera Sensor Gateways, LED lighting etc.



AP-3800 with Developer Module



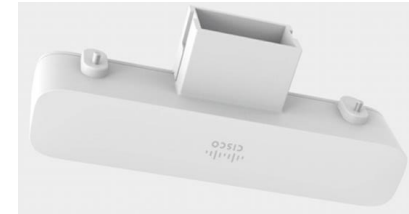
Pixy (CMUcam5) Smart Vision Sensor



Beaglebone



Raspberry Pi



Design on the developer board then create custom modules – AP has filtering for cellular co-existence, can supply power etc.

Module SDK Supported through Devnet

<http://Developer.cisco.com/site/devnet/overview>

3 simple steps to becoming a DevNet member

Step 1

Create a Cisco ID >
(if you don't already have one)

Step 2

Log in to DevNet and create
your account >

Step 3

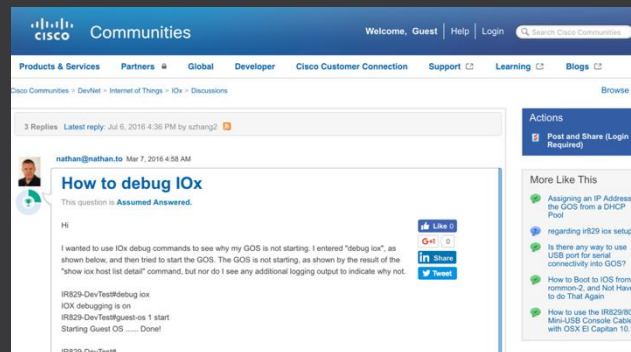
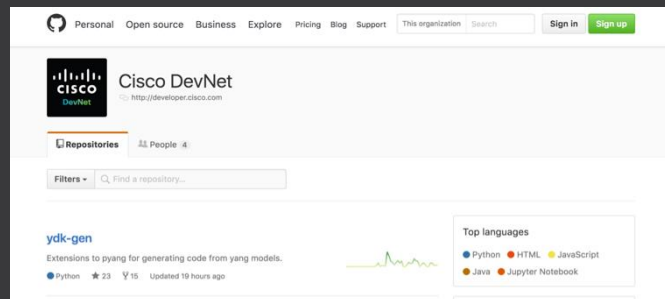
Complete your profile (at any
time) and earn points towards
Cisco DevNet badges.



- ✓ Set your profile to customize your notifications
- ✓ Use the Learning Labs
- ✓ Download APIs and SDKs
- ✓ Get answers on the community forums
- ✓ Access fully-tooled sandboxes
- ✓ Receive loads of support

Devnet provides the following resources...

- ✓ **Sample code & applications on DevNet**
- ✓ **Learning labs and documentation**
- ✓ **Tutorials and demo videos**
- ✓ **DevNet Sandbox – Virtually test code for common use cases**
- ✓ **Community/Forums to help address technical questions**



Agenda

01

Introducing WLC 3504

02

Access Point Update

03

8.5 Software Features

04

Mobility Express Update

Identity PSK

Challenges for Enterprises: Advanced security encryption across all devices



Increased demand for
IoT devices



Identity security
without 802.1x



Simple Operations
High Scale
Cost Effective

Keys Solution Asks:

Private PSK with RADIUS integration; Per client AAA override (VLAN / ACL, QoS etc)

Cisco Advantage:

Highly scalable identity PSK solution designed for a large multi controller network

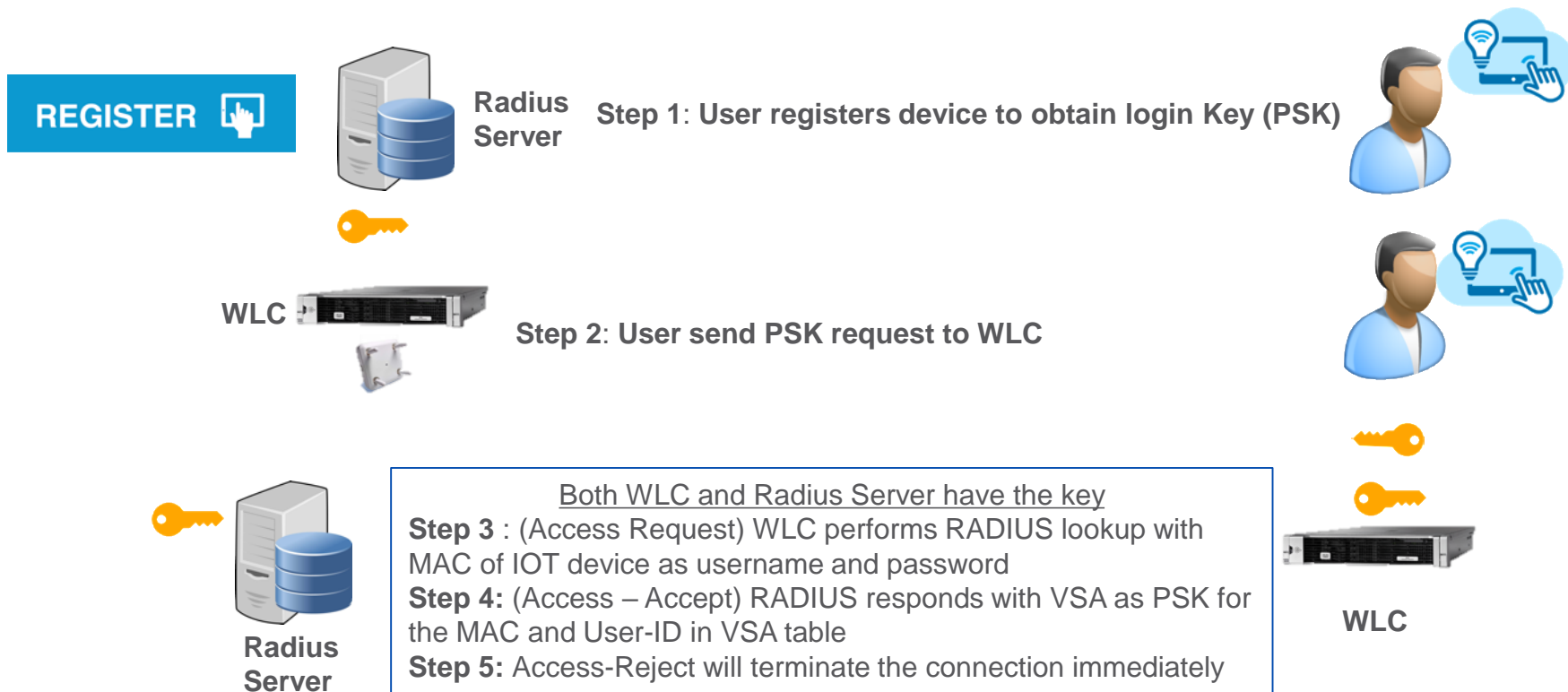
Identity PSK

Why do we need IPSK support?

- All clients joining the WLAN share the same key leading to security issues if keys are shared with unauthorized users
- In case of key compromised on one client leads to changing the key for every client associated to that SSID
- Most of the IoT devices that use PSK do not have 802.1x supplicant
- Leading to the need of supporting keys that are configurable per device

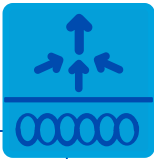
Phase 1 deployment scenario

PSK is assigned on external RADIUS Server



Controller Configuration

- Radius server added globally
- Add the WLAN with PSK Key and enable Mac Filtering
- Enable AAA Override for the WLAN



RADIUS Authentication Servers

Auth Called Station ID Type AP MAC Address:SSID

WLANs > Edit 'IPSK'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name IPSK

Type WLAN

SSID IPSK

WLANs > Edit 'IPSK'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Allow AAA Override ☒ Enabled

Coverage Hole Detection ☒ Enabled

Enable Session Timeout ☐

Airport IE ☒ Enabled

ISE Configuration Example



Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	IPSK-IoT	if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS 18:65:90:b2:a8:11)	then IPSK-Auth

Advanced Attributes Settings

Cisco:cisco-av-pair

=

psk-mode=ascii

Cisco:cisco-av-pair

=

psk=123456789

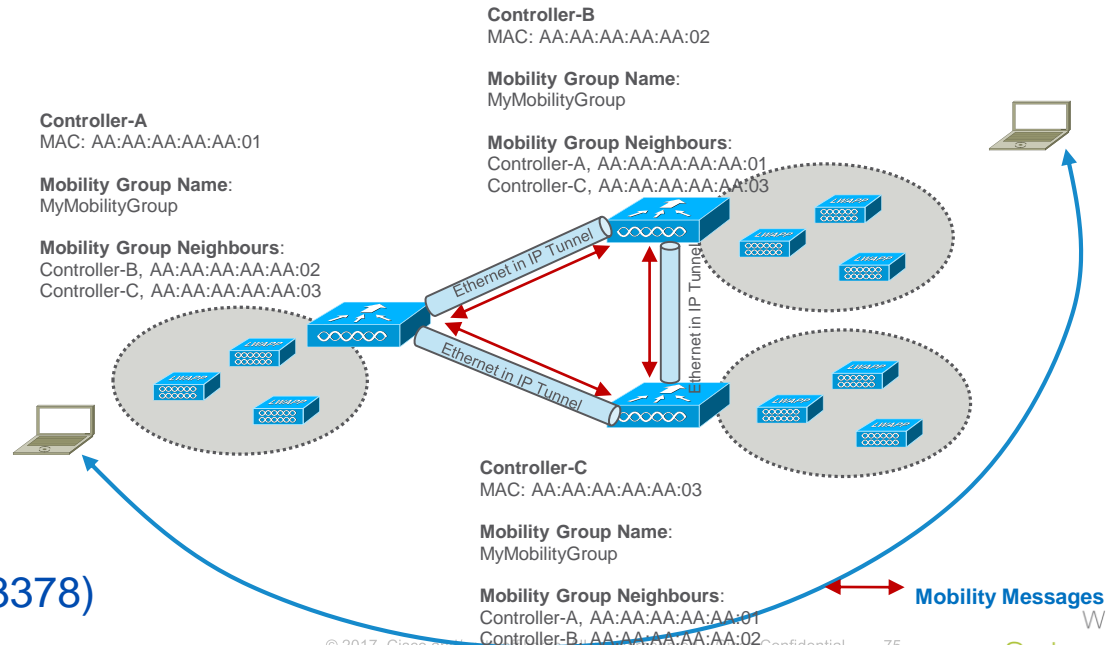
Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=123456789

End to End Encrypted Tunnel between Anchor and Foreign Controllers

Architecture with Mobility Groups prior to 8.5

- Mobility Group allows controllers to peer with each other to support seamless roaming across controller boundaries
- APs learn the IPs of the other members of the mobility group after the CAPWAP Join process
- Support for up to 24 controllers, 24000 APs per mobility group
- Mobility messages exchanged between controllers
- Data tunneled between controllers in EtherIP (RFC 3378)



Anchor to Foreign Encrypted Mobility Tunnels

In release **8.5** end-to-end Tunnel encrypted between Anchor and Foreign Controllers

The encrypted tunnel passes through CAPWAP v4 with DTLS encryption

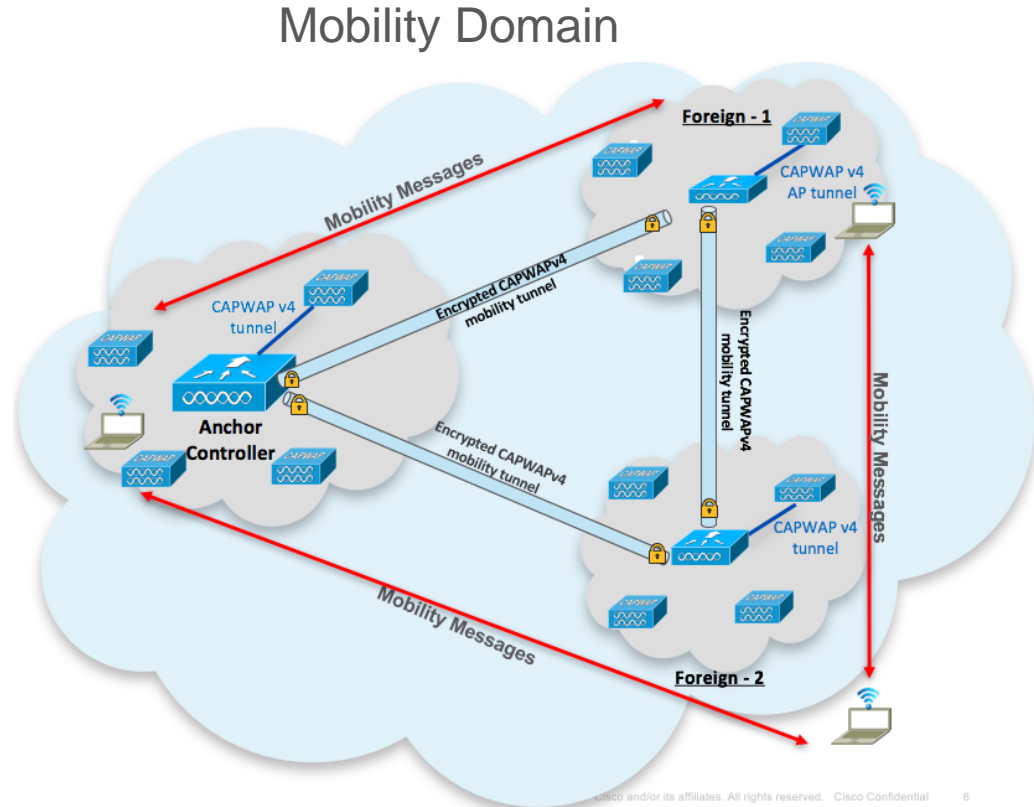
Old Mobility Architecture will be supported

Client SSO will be supported

Supported on 5508, WiSM-2, 3504, 5520 and 8540 controllers



- config mobility encryption enable / disable
- show mobility summary



Apple and ISE Best Practices

Cisco and Apple Best Practices

8.5



APPLE DEVICES

- + WLAN Configuration ☐
- + 5GHz Enabled ☒
- + 5GHz Mandatory Rates ☐
- + 5GHz EDCA Fastlane ☐
- + 5GHz MCS Rates ☒
- + QOS Trust DSCP ☐
- + QOS Platinum Profile ☐
- + mDNS or Bonjour ☐
- + Optimized Roaming Disabled ☒
- Less Optimizations...



Monitoring

Network Summary

Access Points

Clients

Rogues

Access Points

Clients

Interferers

Wireless Dashboard

AP Performance

Client Performance

Best Practices

APPLE DEVICES

WLAN Configuration

None of the Active WLANs are compliant with Cisco Apple Best Practices

Benefits : Allows the user to identify if the WLAN is configured with recommended L2 security, QoS and Advanced settings for Apple devices.

[Learn More...](#)

Detailed

Ignore

+ 5GHz Enabled	<input checked="" type="checkbox"/>
+ 5GHz Mandatory Rates	<input type="checkbox"/>
+ 5GHz EDCA Fastlane	<input checked="" type="checkbox"/>
+ 5GHz MCS Rates	<input checked="" type="checkbox"/>
+ QOS Trust DSCP	<input checked="" type="checkbox"/>
+ QOS Platinum Profile	<input checked="" type="checkbox"/>
+ mDNS or Bonjour	<input type="checkbox"/>
+ Optimized Roaming Disabled	<input checked="" type="checkbox"/>

— Less Optimizations...



WLANs

WLANs

WLANs

Advanced

WLANs

Current Filter: Profile Name: Demo-Mobility2

[\[Change Filter\]](#)[\[Clear Filter\]](#)

Create New



Go

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	2	WLAN	Demo-Mobility2	Demo-Mobility2	Enabled	[WPA2][Auth(802.1X)]	

WLAN Profile

Security

QoS

Advanced

Configuration



Demo-Mobility2



Manual Configuration

Security

QoS

Advanced

✓ Fast Transition should be Enabled or Adaptive

✓ FT PSK has to be enabled

✓ FT 802.1X has to be enabled

✓ Layer 3 Security has to be None

✗ Over the DS has to be disabled

✓ Fastlane should be enabled

✓ QoS has to be Platinum (Voice)

✓ AVC Profile has to be enabled and AUTOQOS-AVCPROFILE applied

✗ WMM Policy should be required

✓ 11k Neighbor List or Dual Band should be enabled

✓ 11v BSS Transition should be enabled

✓ WLAN Radio Policy has to be ALL or 802.11a or 802.11a/g

✗ mDNS Snooping should be enabled

Cisco ISE Best Practices

Monitoring

- Network Summary
 - Access Points
 - Clients
- Rogues
 - Access Points
 - Clients
- Interferers
- Wireless Dashboard
 - AP Performance
 - Client Performance
- Best Practices**

Best Practices List:

- Auto Dynamic Channel Assignment ☒
- Auto Transmit Power Control ☐
- [More Optimizations...](#)
- APPLE DEVICES**
- WLAN Configuration ☐
- 5GHz Enabled ☒
- 5GHz Mandatory Rates ☐
- [More Optimizations...](#)
- ISE RADIUS**
- Radius Server Timeout ☐
- WLAN ISE Configuration ☐
- Radius Aggressive Failover ☒

Message: None of the Active WLANs are compliant with Cisco ISE Best Practices.

Benefits : Allows the user to identify if the WLAN is configured with recommended configuration for Cisco ISE Radius Server.

[Learn More...](#)

[Detailed](#) [Ignore](#)



WLANs

WLANs

WLANs

Advanced

WLANs

Current Filter:

Profile Name: Demo-Mobility2

[\[Change Filter\]](#)[\[Clear Filter\]](#)

Create New



Go

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	2	WLAN	Demo-Mobility2	Demo-Mobility2	Enabled	[WPA2][Auth(802.1X)]	

WLAN Profile

☒ Demo-Mobility2

Security

Advanced

Manual Configuration



- ✓ Interim Update in AAA Server should be enabled
- ✓ Interim Interval in AAA Server should be 0 Second

- ✓ Session Timeout should be enabled
- ✗ Session Timeout should be greater than or equal to 7200 Seconds
- ✗ Client Exclusion has to be enabled
- ✗ Client Exclusion value has to be set to 180 Seconds
- ✗ Client user idle timeout should be enabled
- ✗ Client user idle timeout should not be greater than 3600 Seconds

vWLC on AWS

Why install AireOS on AWS?



Full capabilities of AireOS 8.5

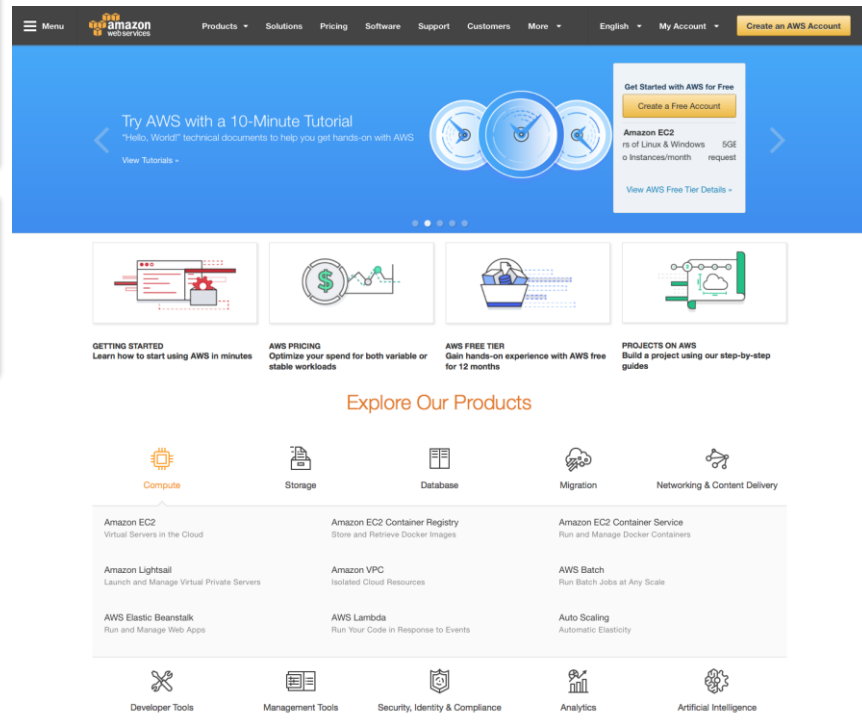
Available for partners to host

Host your own private cloud

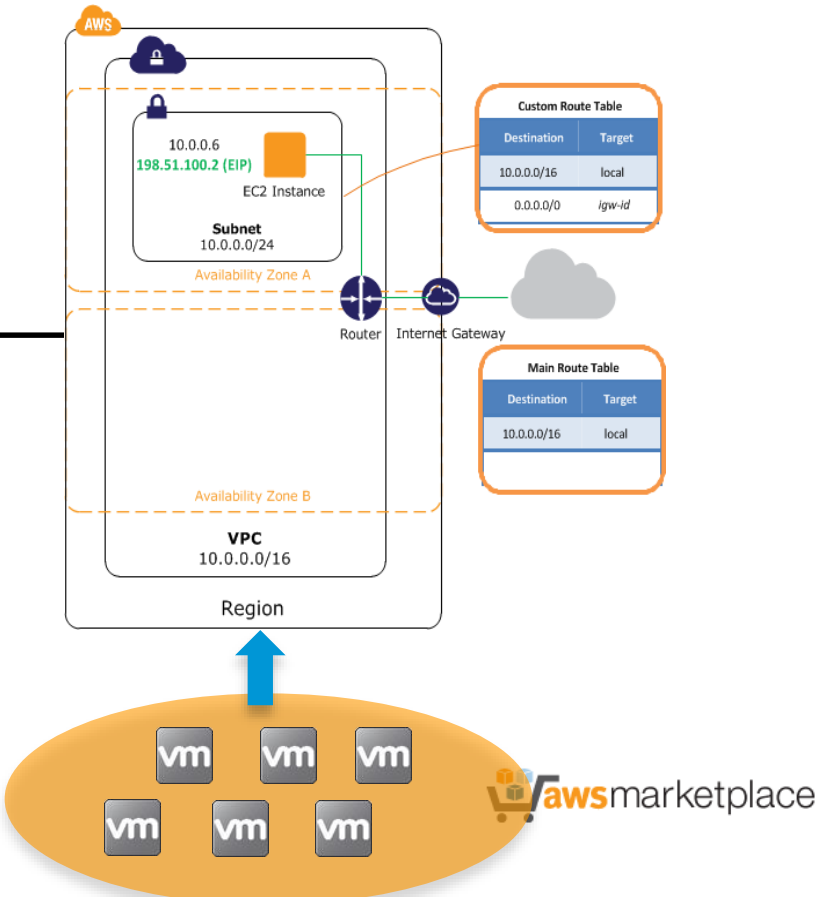
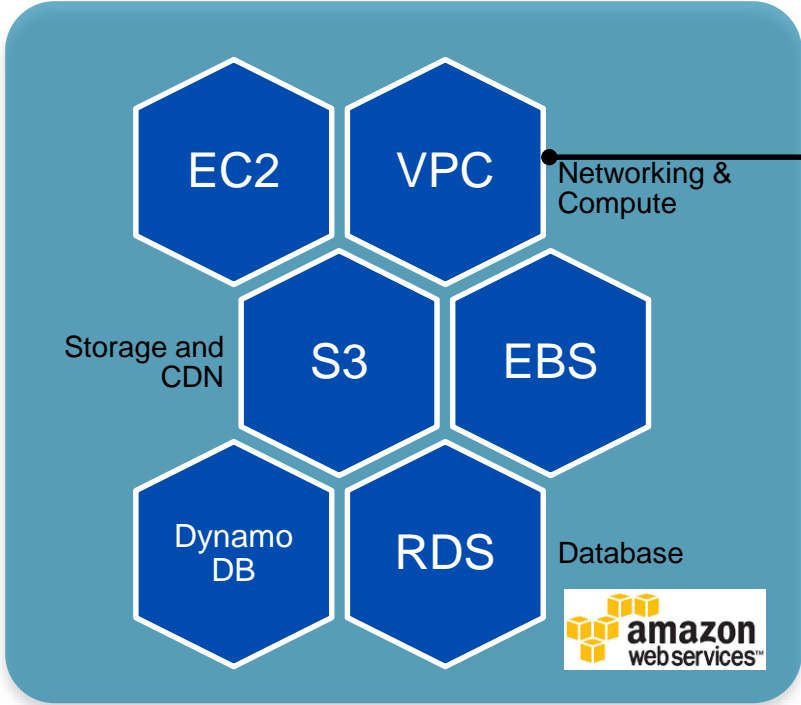
Flex connect mode

Application Visibility and Control

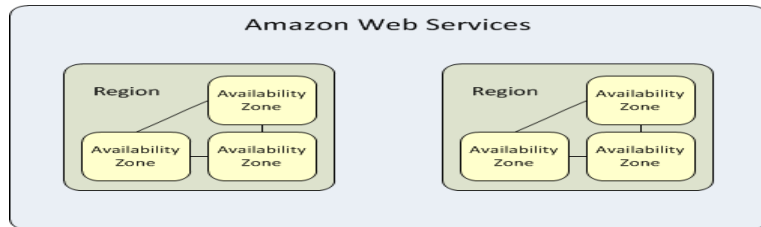
REST API for Orchestration



Amazon Web Services



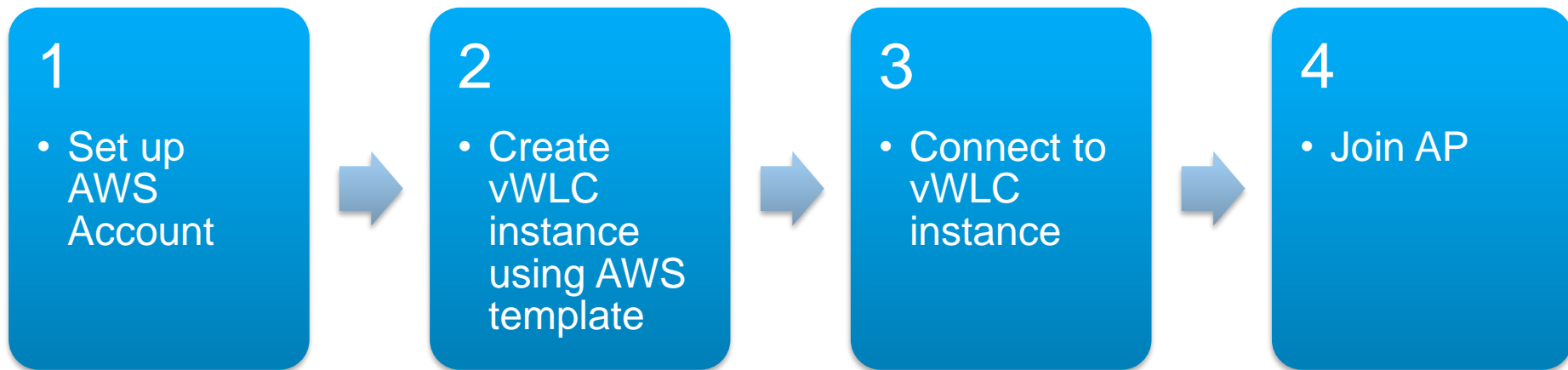
Amazon VPC key components



Regions and Availability zones

- EC2 is hosted in multiple data centers across the world. A Region is a separate geographic area. Regions are not connected.
- EC2 instances have to be launched into a specific region. Locating your EC2 instances close to the end users can reduce latency
- Regions available are Tokyo, Singapore, Sydney, Ireland, Sao Paulo, US East (N. Virginia), US West (North Cal.), US West (Oregon), *GovCloud*** (for US government sensitive workloads only)
- Multiple isolated regions within a Region are called Availability Zones (they are inter-connected using low latency links).

Steps to deploy the vWLC in AWS



CloudFormation Stack Template

- Text file to create vWLC instance with required resources (type small/large)
- Specifies AMI and region for use
- Assigns a public IP that can be used to access the instance over the internet.
- Uses two separate subnets for service and management port

```

"Parameters" : {
  "InstanceType" : {
    "Description" : "vWLC EC2 instance type",
    "Type" : "String",
    "Default" : "c3.2xlarge",
    "AllowedValues" : [ "m4.large", "m4.xlarge", "m4.2xlarge" ],
    "ConstraintDescription" : "must be a valid SRI0v EC2 instance type"
  },
  "Mappings" : {
    "AWSRegion2AMI" : {
      "us-east-1" : { "AMI" : "ami-893af29f" }
    }
  },
  "Outputs" : {
    "InstanceId" : {
      "Value" : { "Ref" : "EC2Instance" },
      "Description" : "Instance Id of newly created instance"
    },
    "EIP1" : {
      "Value" : { "Fn::Join" : [ " ", [ "IP address", { "Ref" : "EC2Instance" } ] ] },
      "Description" : "Primary public IP address for Eth1"
    },
    "PrimaryPrivateIPAddress" : {
      "Value" : { "Fn::Join" : [ " ", [ "IP address", { "Fn::GetAtt" : [ "EC2Instance", "PrivateIpAddress" ] } ] ] },
      "Description" : "Primary private IP address of Eth1"
    }
  }
}

```

vWLC Instance

Instance: **i-004417e74b1aa8bb6 (vWLC)** Elastic IP: **34.206.255.12**

Description

Status Checks

Monitoring

Tags

Instance ID

i-004417e74b1aa8bb6

Instance state

running

Instance type

c3.2xlarge

Elastic IPs

[34.206.255.12*](#)

Availability zone

us-east-1b

Security groups

[vWLC_SG](#) . [view inbound rules](#)

Scheduled events

[No scheduled events](#)

AMI ID

[Large_VWLC_AMI-balamura. \(ami-893af29f\)](#)

Platform

-

IAM role

-

Key pair name

-

Owner

768218550934

Launch time

March 1, 2017 at 5:25:51 PM UTC-8 (310 hours)

Termination protection

False

Lifecycle

normal

Public DNS (IPv4)

-

IPv4 Public IP

[34.206.255.12](#)

IPv6 IPs

-

Private DNS

ip-172-31-18-131.ec2.internal

Private IPs

172.31.18.131, 172.31.33.47

Secondary private IPs

VPC ID

vpc-33c08854

Subnet ID

subnet-7280675f

Network interfaces

[eth0](#)
[eth1](#)

Source/dest. check

True

EBS-optimized

False

Root device type

ebs

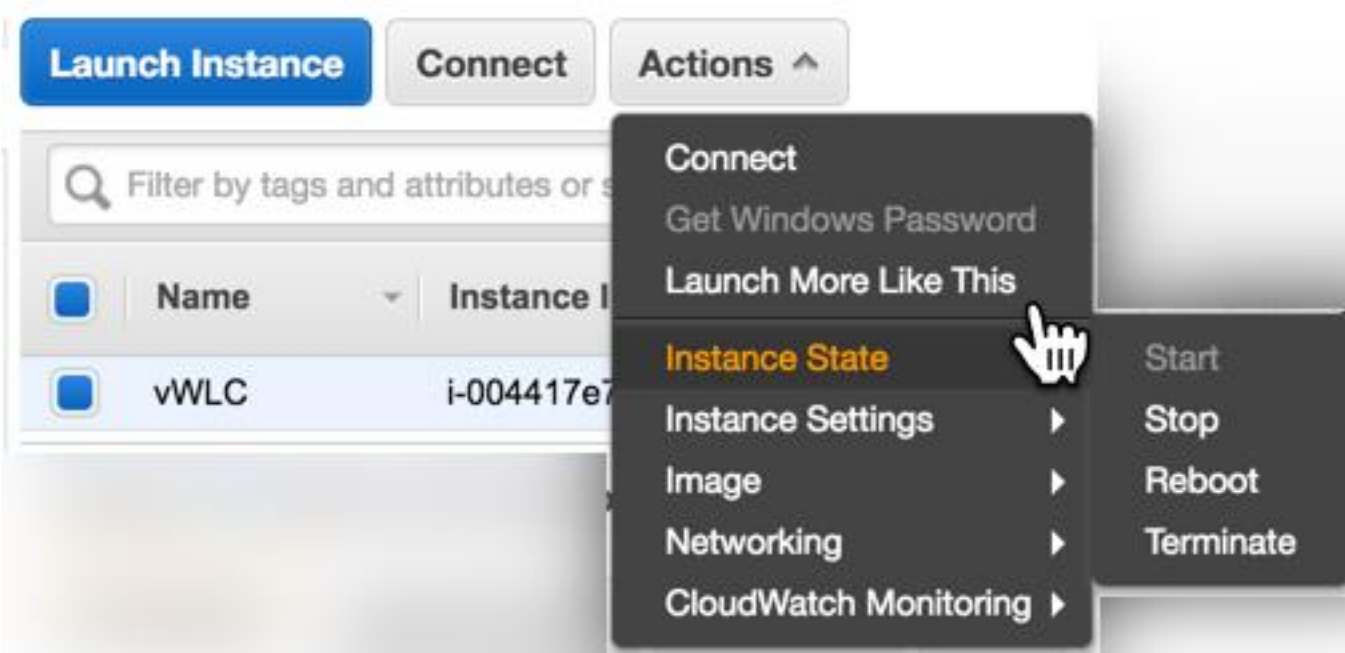
Root device

[/dev/sda1](#)

Block devices

[/dev/sda1](#)

Managing vWLC Instance



vWLC Instance Access



The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with 'Services', 'Resource Groups', and a user profile 'Paul Nguyen'. On the left, a sidebar lists 'EC2 Dashboard', 'Events', 'Tags', 'Reports', and 'Limits'. The main area displays a table of EC2 instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), and IPv4 Public IP. One instance is listed: 'vWLC' with ID 'i-004417e74b1aa8b...', type 'c3.2xlarge', in 'us-east-1b' zone, state 'running', and public IP '34.206.255.12'. Above the table are buttons for 'Launch Instance', 'Connect', and 'Actions'. A search bar is also present.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
vWLC	i-004417e74b1aa8b...	c3.2xlarge	us-east-1b	running	2/2 checks ...	None		34.206.255.12

```
PC:~ xy$ ssh 34.206.255.12
The authenticity of host '34.206.255.12 (34.206.255.12)' can't be established.
ECDSA key fingerprint is SHA256:xFiShkFWmgMIm/PbiQfDVmJaSp0YgTuLeheqCX+Qqp.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '34.206.255.12' (ECDSA) to the list of known hosts.
```

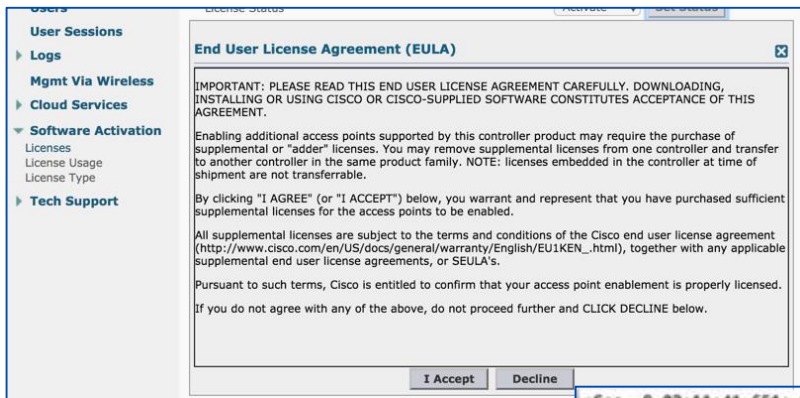
```
(Cisco Controller)
User: cisco
Password:*****
(Cisco Controller) >
```



The screenshot shows the Cisco Wireless LAN Controller login page. It features the Cisco logo at the top, followed by the title 'Wireless LAN Controller'. Below the title, a welcome message says 'Welcome! Please click the login button to enter your user name and password'. At the bottom, there is a green 'Login' button with a hand cursor icon pointing to it. The page is framed by a blue border.

Worldwide
Sales Training

Activate License / Join APs



```
*Sep 9 02:11:41.651: %CAPWAP-6-AP_IMG_DWNLD: Required!
extracting info (327 bytes)
Image info:
  Version Suffix: k9w8-.v153_3_jd.201607162332
  Image Name: ap3g2-k9w8-mx.v153_3_jd.201607162332
  Version Directory: ap3g2-k9w8-mx.v153_3_jd.201607162332
  Ios Image Size: 12851712
  Total Image Size: 15022592
  Image Feature: WIRELESS LAN|LWAPP
  Image Family: AP3G2
  Wireless Switch Management Version: 8.3.90.59
MwarVersion:08035A3B.First AP Supported Version:07060000.

Image version check passed

Extracting files...
ap3g2-k9w8-mx.v153_3_jd.201607162332/ (directory) 0 (bytes)
extracting ap3g2-k9w8-mx.v153_3_jd.201607162332/8004.img (569225 bytes) image not found on AP. Downloading image from Controller.
*Sep 9 02:11:41.655: Loading file /ap3g2...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

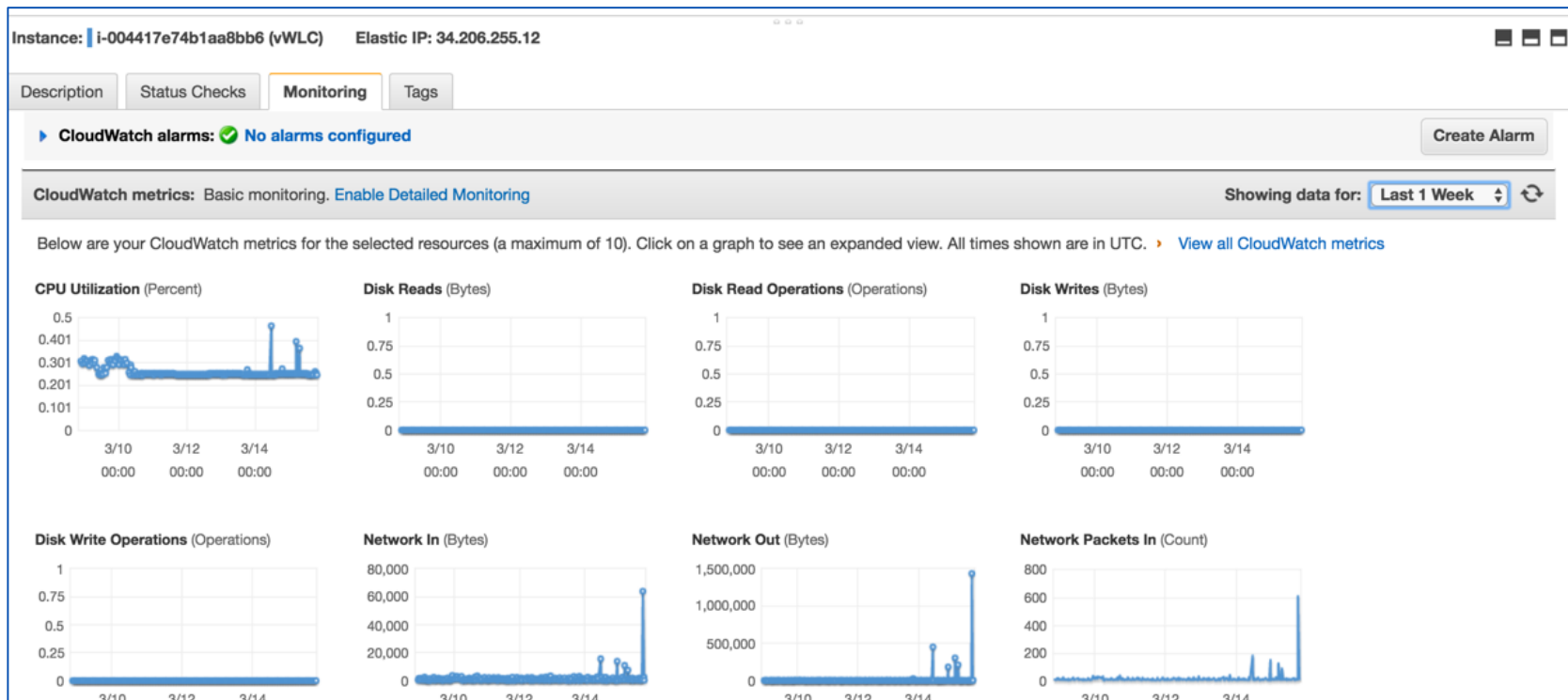

Backup of vWLC Instance

The screenshot displays the AWS Management Console interface. On the left, the navigation menu includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES', 'IMAGES', 'ELASTIC BLOCK STORE', and 'NETWORK & SECURITY'. The 'INSTANCES' section is expanded, showing 'Instances', 'Spot Requests', 'Reserved Instances', 'Scheduled Instances', and 'Dedicated Hosts'. The 'ELASTIC BLOCK STORE' section is also expanded, showing 'Volumes' and 'Snapshots'. The 'Snapshots' page is active, showing a table with columns 'Name', 'Snapshot ID', 'Size', and 'Description'. A 'Create Snapshot' button is visible at the top. A mouse cursor is clicking on the 'Create Snapshot' button. A modal dialog box titled 'Create Snapshot' is open, showing the following fields:

- Volume**: vol-0d9c7c87eed1e14d4
- Name**: vWLC-snapshot
- Description**: Backup for vWLC Instance
- Encrypted**: No

At the bottom right of the dialog, there are 'Cancel' and 'Create' buttons.

Monitoring vWLC Instance with CloudWatch



vWLC Alarm with CloudWatch

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☒ **Send a notification to:** CPU_High_Alarm [cancel](#)

With these recipients: paul@cisco.com

☐ **Take the action:**

- ☐ Recover this instance ⓘ
- ☐ Stop this instance ⓘ
- ☐ Terminate this instance ⓘ
- ☐ Reboot this instance ⓘ

Whenever: Average of CPU Utilization

Is:


For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awsec2-i-004417e74b1aa8bb6-CPU-Utilization

[Cancel](#) [Create Alarm](#)

CPU Utilization Percent

Time	CPU Utilization Percent
3/15 14:00	~0
3/15 16:00	~0
3/15 18:00	~0


CISCO

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

95

Worldwide
Sales Training

Agenda

01

Introducing WLC 3504

02

Access Point Update

03

8.4 / 8.5 Software Features

04

Mobility Express Update

Agenda – Cisco Mobility Express

01

Quick recap of Cisco Mobility Features

- Release 8.4 Highlights
-

02

Release 8.5 Features

- Simplified Day 0
 - Conversion - Simplified in Day 1
 - Support for Fastlane in UI
 - TACACS+ and RADIUS Support for Admin Accounts
 - ACL Enhancements
 - Support for Configuring External Antennas
-

03

Release 8.5 Manage Service Provider Features

- CALEA
- Passpoint
- Support for centralized NAT on Guest WLANs

Agenda – Cisco Mobility Express

01

Quick recap of Cisco Mobility Features

- Release 8.4 Highlights
-

02

Release 8.5 Features

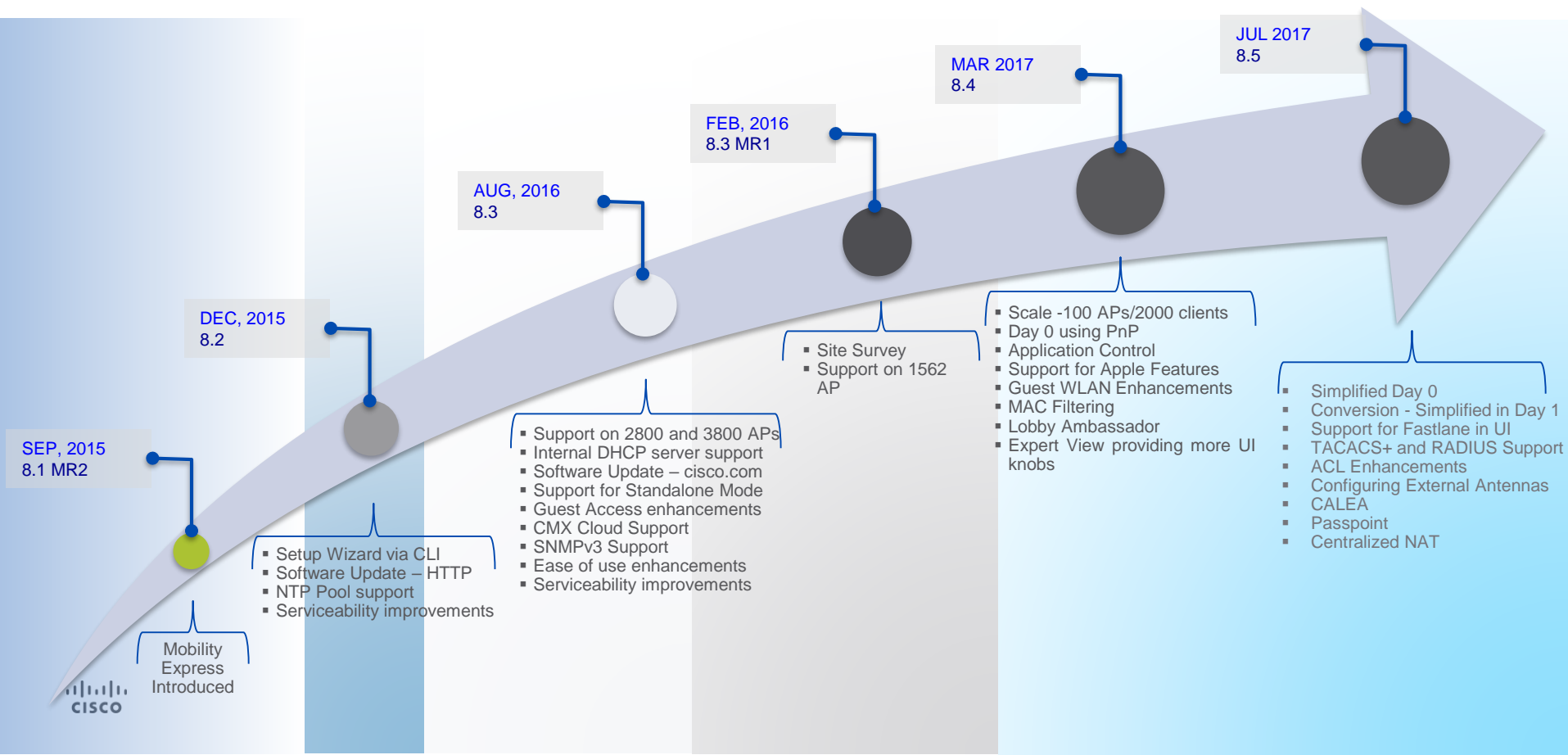
- Simplified Day 0
 - Conversion - Simplified in Day 1
 - Support for Fastlane in UI
 - TACACS+ and RADIUS Support for Admin Accounts
 - ACL Enhancements
 - Support for Configuring External Antennas
-

03

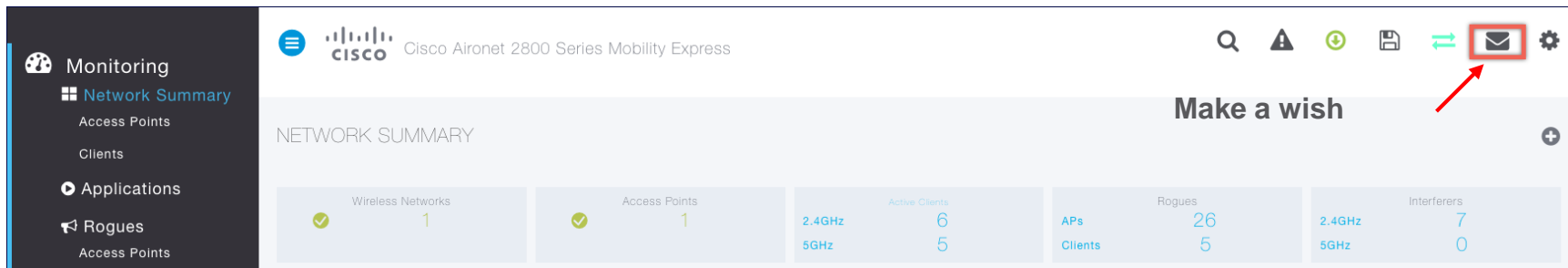
Release 8.5 Manage Service Provider Features

- CALEA
- Passpoint
- Support for centralized NAT on Guest WLAN

Evolution of Cisco Mobility Express Solution

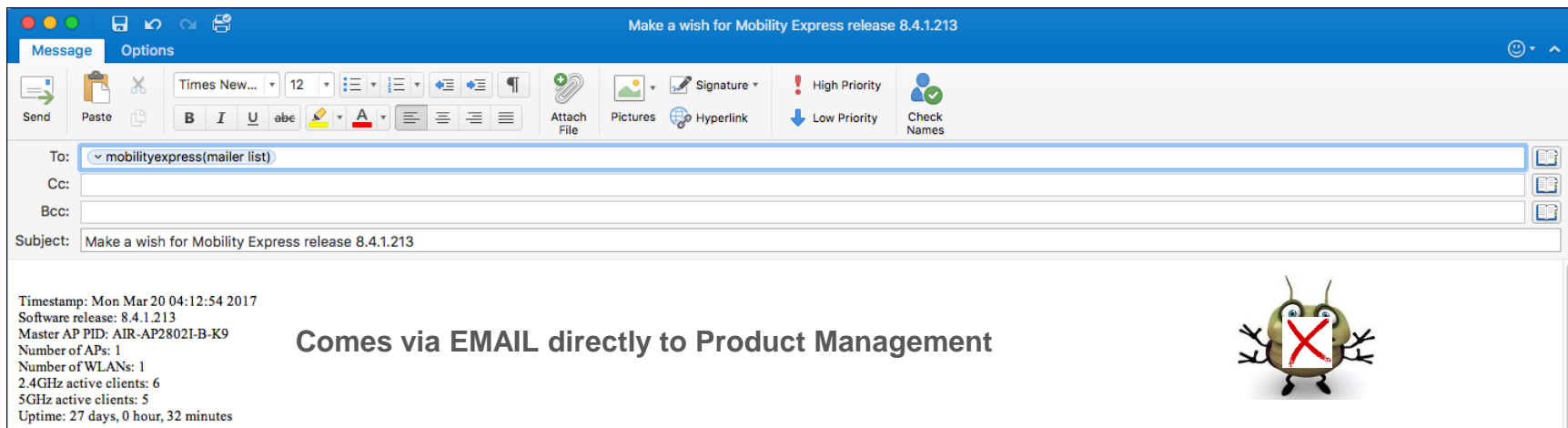


Feedback is important!!



The dashboard shows the following metrics:

Category	Value
Wireless Networks	1
Access Points	1
Active Clients	6
2.4GHz	6
5GHz	5
APs	26
Clients	5
Rogues	7
Interferers	0
2.4GHz	7
5GHz	0



Message Options

Make a wish for Mobility Express release 8.4.1.213

To: mobilityexpress(mailer list)

Cc:

Bcc:

Subject: Make a wish for Mobility Express release 8.4.1.213

Timestamp: Mon Mar 20 04:12:54 2017
 Software release: 8.4.1.213
 Master AP PID: AIR-AP2802I-B-K9
 Number of APs: 1
 Number of WLANs: 1
 2.4GHz active clients: 6
 5GHz active clients: 5
 Uptime: 27 days, 0 hour, 32 minutes

Comes via EMAIL directly to Product Management

Which Access Points can run Mobility Express?





stay on top

Worldwide
Sales Training

