

Understand the FlexConnect Feature Matrix for AireOS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[FlexConnect](#)

[FlexConnect Feature Matrix - Legacy and New Features in Release 7.0.116 and Later](#)

[Security - Client](#)

[Security - Infrastructure](#)

[Security](#)

[Voice & Video](#)

[Services](#)

[Infrastructure](#)

[Mobility / Roaming Scenarios](#)

[Related information](#)

Introduction

This document describes the feature matrix for the FlexConnect feature on the Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Control and Provisioning of Wireless Access Points (CAPWAP) protocol
- Configuration of lightweight Access Points (APs) and Cisco WLCs

Components Used

The information in this document is based on CUWN Releases 7.0.116.0 and later. This article has been updated with Release 8.8

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

FlexConnect

FlexConnect is a wireless solution for branch office and remote office deployments. It enables you to configure and control APs in a branch or remote office from the corporate office through a WAN link without the deployment of a controller in each office. The FlexConnect APs can switch client data traffic locally and perform client authentication locally. When they are connected to the controller, they can also send traffic back to the controller. FlexConnect is only supported on these components:

- 700, 1130AG, 1140, 1240AG, 1250, 1700, 1810, 1815, 1830, 1840, 1850, AP801, 1600, 1700, 2600, 2700,2800, 3500I, 3500E, 3600, 3700, 3800, 1040, 1520, 1530, 1550, 1560,1570, and 1260 APs
- Cisco Flex 8500 and 7500, Cisco 5500, 3504,vWLC, and 2500 Series Controllers
- Catalyst 3750G Integrated WLC Switch
- Cisco WiSM and WiSM2
- Controller Network Module for Integrated Services Routers

FlexConnect local authentication is useful where you cannot maintain a remote office setup with a minimum bandwidth of 128 kb/s and a round-trip latency of no greater than 100 ms. The maximum tolerated latency for FlexConnect is 300 ms, regardless of the features that are used.

The next section outlines the FlexConnect Feature Matrix.

Note: Pre-802, 11n APs, such as 1130 or 1240, are still supported by later code. However, these APs do not receive new features as of Release 7.3. Therefore, these APs do not support FlexConnect features that appear after Release 7.3. Similarly, first generation 802.11n APs do not have any of the FlexConnect features of the 8.1 feature set even if they are able to join such a WLC. Refer to the release notes for more information.

Note: 802.11ac wave 2 APs and Catalyst APs are covered by this document which supersedes this matrix which focuses only on AireOS releases :
https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html

FlexConnect Feature Matrix - Legacy and New Features in Release 7.0.116 and Later

Security - Client

Security support on FlexConnect varies with different modes and states. This table summarizes the security features that are supported:

	WAN Up (Central Switching)	WAN Up (Local Switching)	WAN Up (Local Switching, Local Authentication)	WAN Down (Standalone)
Open/Static WEP	Yes	Yes	Yes	Yes
WPA-PSK	Yes	Yes	Yes	Yes
802.1x (WPA/WPA2)	Yes	Yes	Yes	Yes
MAC filter Authentication	Yes	Yes	No	No
CCKM Fast Roaming	Yes	Yes	No	Yes, for connected clients. No, for new clients.

Security - Infrastructure

	WAN Up (Central Switching)	WAN Up (Local Switching)	WAN Down (Standalone)
Data DTLS Encryption	Yes	N/A	N/A
Local EAP (7.0 to 7.4)	Yes (LEAP/EAP-FAST)	Yes (LEAP/EAP-FAST)	Yes (LEAP/EAP-FAST)
Local EAP (7.5 and later)	Yes (LEAP/EAP-FAST/PEAP/EAP-TLS)	Yes (LEAP/EAP-FAST/PEAP/EAP-TLS)	Yes (LEAP/EAP-FAST/PEAP/EAP-TLS)
Backup Radius	Yes (7.0.116)	Yes (7.0.116)	Yes
MIC	Yes	Yes	Not applicable

Security

Security support on FlexConnect varies with different modes and states. This table summarizes the legacy and new security features supported with WLC Release 7.0.116.0 and later:

	WAN Up (Central Switching)	WAN Up (Local Switching)	WAN Up (Local Switching, Local Authentication)	WAN Down (Standalone)
Adaptive Wireless Intrusion Prevention (aWIPS)	Yes	Yes	Yes	No
Rogue, Intrusion Detection (IDS)	Yes	Yes	Yes	No
Management Frame Protection (MFP) (Client, Infrastructure)	Yes	Yes (no for wave 2 APS)	Yes (no for wave 2 APS)	No
802.11w "MFP"	Yes (7.5)	Yes (7.5)	Yes (7.5)	Yes (7.5)
802.11r Fast Transition	Yes	Yes	No	No
Self-Signed Certificate (SSC)	Yes	Yes	Yes	N/A
Rogue Location Discovery Protocol (RLDP)	can work, depends on hops, WAN speed	can work, depends on hops, WAN speed (no for wave 2 APS)	can work, depends on hops, WAN speed (no for wave 2 APS)	No
Opportunistic Key Caching (OKC) Fast Roam	Yes	Yes	Yes	No ⁽¹⁾
FlexConnect Local Auth	N/A	Yes	Yes	Yes
Ipv4 AAA Override	Yes	Yes	Yes	Yes
Ipv6 AAA override	Yes	Yes ⁽⁵⁾	Yes ⁽⁵⁾	Yes ⁽⁵⁾

AAA VLAN assignment per FlexGroup with VLAN name	N/A	Yes (8.1)	Yes (8.1)	Yes (8.1)
Static ACL	Yes	Yes ⁽²⁾ No	Yes ⁽²⁾ No	Yes ⁽²⁾ No
Per-user radius ACL ⁽⁴⁾	Yes (7.5)	Yes (7.5)	Yes (7.5)	No
L2 ACL	Yes (7.5)	Yes (7.5)	Yes (7.5)	Yes (7.5)
DNS ACL	Yes (7.6)	No	No	No
P2P Blocking	Yes	Yes	Yes	Yes
Mesh LSC	N/A	N/A	N/A	N/A
Bring Your Own Device /ISE(BYOD)	Yes	Yes (7.2.110.0)	No	No
PCI Compliance for Neighbor Pkts	Yes	Yes	Yes	No
Russia DTLS Support	Yes	N/A	No	No
wIPS Enhanced Local Mode (ELM)	Yes	Yes	Yes	No
Limit Clients per WLAN	Yes	Yes ⁽³⁾	Yes	No
Limit Clients per Radio	Yes	Yes	Yes	Yes
Client Exclusion Policy	Yes	Yes ⁽³⁾	Yes	No
Radius NAC	Yes	Yes	No	No
TrustSec SXP at AP level	Yes (8.4)	Yes (8.4)	Yes (8.4)	Yes (8.4)
TrustSec SXP at WLC	Yes (8.3)	Yes (8.3)	Yes (8.3)	Yes (8.3)
Identity PSK	Yes (8.5)	Yes(8.5)	No	Yes(8.5)
Identity PSK with P2P blocking	Yes (8.8)	Yes (8.8)	No	No
AAA-enforced Policy and quota management	Yes (8.8)	Yes (incl. Flex +Bridge) (8.8)	No	No

(1) Yes for clients that have association at Connected mode.

(2) FlexConnect Access Control Lists (ACLs) must be used. Note that flex ACLs are not supported on the AP native VLAN!

(3) Limits/exclusion done by WLC so client is deauthorized after a successful Association Response.

(4) Note that the per-user ACL on FlexConnect does not override a VLAN ACL on flex AP like it would override a WLAN ACL on local mode AP. If both per user-ACL is pushed and AAA-VLAN ACL configured on the flex group, both take effect.

(5)With FlexConnect local switching, Multicast is forwarded only for the VLAN that the SSID is mapped to and not to any overridden VLANs. Therefore, IPv6 does not work as expected because Multicast traffic is forwarded from the incorrect VLAN. Therefore vlan assignment is not supported on local switching with ipv6

Note: At any given point, an AP has a maximum of 16 VLANs. First, the VLANs are selected as per

the AP configuration (WLAN-VLAN), and then the remaining VLANs are pushed from the FlexConnect group in the order that they are configured or displayed in the FlexConnect group. If the VLAN slots are full, an error message is displayed

Voice & Video

This table lists the legacy and new Voice & Video services supported with WLC Release 7.0.116.0 and later with FlexConnect:

	WAN Up (Central Switching) 100 ms RTT	WAN Up (Local Switching) 100 ms RTT	WAN Down (Standalone)
Voice	Yes with RTT 100 ms	Yes with RTT 100 ms Yes with RTT 900 ms (with CCKM and OKC)	Yes with RTT 100 ms Yes with RTT 900 ms (with CCKM and OKC)
QoS Markings ⁽¹⁾	Yes	Yes	Yes
QoS Per-User Bandwidth Contract	Yes (7.4)	Yes (7.5)	No
UAPSD	Yes	Yes	Yes
Voice Diagnostics	Yes	Yes	No
Voice Metrics	Yes	Yes	No
TSPEC /Call Admission Control (CAC)	Yes - non CCX Yes - CCX ⁽²⁾	Yes - non CCX Yes - CCX ⁽²⁾	No
<p>(1) Includes both DSCP/dot1p markings. (2) CAC on WLC, deauthorization on roaming failure.</p>			

Services

This table lists the legacy and new services supported with WLC Release 7.0.116.0 and later with FlexConnect:

	WAN Up (Central Switching)	WAN Up (Local Switching)	WAN Up (Local Switching, Local Authentication)	WAN Down (Standalone)
Internal Webauth	Yes	Yes	No	N/A
External Webauth	Yes (7.2.110.0)	Yes (7.2.110.0)	No	N/A
CleanAir (SI on 3500)	Yes	Yes	Yes	N/A
Multicast-Unicast (Videostream)	Yes (except on 7500, 8500 and vWLC)	Yes (8.0) (not on wave 2 APs)	Yes (8.0) (not on wave 2 APs)	Yes (8.0) (not on wave 2 APs)
Location	Yes with BW/Scale limitation	Yes with BW /Scale limitation	Yes with BW /Scale limitation	N/A
Radio Ressource Management	Yes	Yes	Yes	No

NG RRM - RF Static Grouping	Yes ⁽¹⁾	Yes ⁽¹⁾	Yes	No
SE Connect (Cleanair Update)	Yes	Yes	Yes	No ⁽²⁾
S60 Enhancement	Yes	Yes	Yes	No
Profiling	Yes	Yes (if you enabled Central DHCP Processing)	Yes (if you enabled Central DHCP Processing)	No
AVC ³	Yes (7.4)	Yes (8.1)	Yes (8.1)	No
Bonjour Gateway	Yes	No	No	No
mDNS AP	Yes	No	No	No
LSS	Yes	No	No	No
Origin Based services	Yes	No	No	No
Priority MAC	Yes	No	No	No
Bonjour Browser	Yes	No	No	No
Flex+Bridge mode	Yes (8.0 but 8.8 for wave2)	Yes (8.0 but 8.8 for wave2)	Yes (8.0 but 8.8 for wave2)	Yes (8.0 but 8.8 for wave2)

(1) Any RRM-specific requirements apply (at least 4 APs for TPC).

(2) Yes for standalone after disconnection from WLC, but no for reboot.

(3) FlexConnect AVC supported on all WLCs (which include vWLC) except 2504.

Infrastructure

	WAN Up (Central Switching)	WAN Up (Local Switching)	WAN Down (Standalone)
Passive Clients	No	Yes	Yes
Proxy ARP	Yes (8.0) (8.3mr1 for wave 2 APs)	Yes (8.0) (8.3mr1 for wave 2 APs)	Yes (8.0) (8.3mr1 for wave 2 APs)
Syslog	Yes	Yes	Yes
CDP	Yes	Yes	Yes
Client Link	Yes	Yes	Yes ⁽²⁾
Load Balancing ⁽³⁾	Yes (7.4)	Yes (7.4)	No
Band Select	Yes	Yes	No
AP Image PreDownload	Yes	Yes	No
FlexConnect Smart AP Image Upgrade	Yes	Yes	Yes ⁽¹⁾
AP Regularity Domain Updates (Chile)	Yes	Yes	Yes
VLAN Pooling/Mcast Optim.	Yes	N/A	N/A
Mesh - 24 backhaul	N/A	N/A	N/A
Cisco WGB Support	Yes	Yes (7.3) (no for wave	Yes (7.3) (no for wave 2

		2 APS)	APS)
3rd party WGB Support	Yes	Yes	Yes
Web Auth Proxy	Yes	Yes	No
FlexConnect AP Group Increase	Yes	Yes	Yes
Client fault tolerance	N/A	Yes	N/A
DHCP Option 60	Yes	Yes	Yes
DFS/802.11h	Yes	Yes	Yes
AP Group VLANs	Yes	N/A	N/A
Vlan mappings through FlexGroups	Yes	Yes	Yes
vlan-based central switching	Yes (8.5 for wave2 APs, 7.3 for IOS APs)	Not applicable	Not applicable
AP LAG	Yes (8.8)	Yes (8.8)	Yes (8.8)

The passive client feature is not supported on Flex APs. However, the APs do not do proxy ARP by default on FlexConnect (and that is a part of the passive client feature). On the contrary, proxy ARP was added as a feature for FlexConnect APs with Release 8.0 and later.

(1) Provided if the Lead AP is already upgraded and member APs are updated with their Lead AP.

(2) Only on second generation 11n APs and later (1600, 2600, 3600, and so on).

(3) FlexConnect APs do not send (re)association responses with status 17 for load-balancing as do Local mode APs; instead, they first send (re)association responses with status 0 (success) and then death with reason 5. This occurs as the AP handles the association locally and load-balancing decisions are taken at the WLC.

Mobility / Roaming Scenarios

WLAN Configuration	Local Switching			Central Switching		
	CCKM	PMK (OKC)	Others	CCKM	PMK (OKC)	Others
Mobility Between Same Flex Group	Fast Roam ⁽¹⁾	Fast Roam ⁽¹⁾	Full Auth ⁽¹⁾	Fast Roam	Fast Roam	Full Auth
Mobility Between Different Flex Group	Full Auth	Fast Roam	Full Auth	Full Auth	Fast Roam	Full Auth
Inter Controller Mobility	N/A	N/A	N/A	Full Auth	Fast Roam	Full Auth

(1) Provided WLAN is mapped to the same VLAN (same subnet). If WLAN is mapped to different subnets, no fast roaming can occur as the client has to obtain a new IP address.

Note: FT/802.11r fast roaming also requires APs to be in the same FlexGroup. Only WPA2 OKC, which happens at the WLC level, can tolerate APs to be in different FlexConnect groups for fast roaming.

Note: In order to support centralized access control through a centralized Authentication, Authorization, and Accounting (AAA) server, such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis with the use of AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller, and the WLAN must be configured with the AAA Override feature enabled. The AAA attribute for an IPv6 ACL is **Airespace-IPv6-ACL-Name**, similar to the **Airespace-ACL-Name** attribute used in order to provision an IPv4-based ACL. The AAA attribute-returned contents must be a string that is equal to the name of the IPv6 ACL, as configured on the controller.

Related information

- [H-Reap Design and Deployment Guide](#)
- [Hybrid Remote Edge Access Point \(H-REAP\) Basic Troubleshooting](#)
- [Technical Support & Documentation - Cisco Systems](#)