

Versions recommandées de Cisco IOS XE pour les contrôleurs LAN sans fil Catalyst 9800

Table des matières

[Introduction](#)

[Fond](#)

[Versions recommandées par le TAC](#)

[IOS XE 17.14.1](#)

[IOS XE 17.13.1](#)

[Dublin 17.12](#)

[17.12.3](#)

[17.12.2](#)

[Dublin 17.11.1](#)

[Dublin 17.10.1](#)

[Cupertino 17.9](#)

[17.9.5](#)

[17.9.4 bis](#)

[17.9.4](#)

[17.9.3](#)

[17.9.2](#)

[17.9.1](#)

[Cupertino 17.8.1](#)

[Cupertino 17.7.1](#)

[Bengaluru 17.6](#)

[17.6.7](#)

[17.6.6 bis](#)

[17.6.6](#)

[17.6.5](#)

[17.6.4](#)

[17.6.3](#)

[17.6.2](#)

[17.6.1](#)

[Bengaluru 17.5.1](#)

[Bengaluru 17.4.1](#)

[Amsterdam 17.3](#)

[17.3.7](#)

[17.3.6](#)

[17.3.5b](#)

[17.3.5 bis](#)

[17.3.4c](#)

[17.3.4](#)

[17.3.3](#)

[17.3.2a](#)

[17.3.1](#)

[Amsterdam 17.2.1](#)

[Amsterdam 17.1.1](#)

[Gibraltar 16.12](#)

[Gibraltar 16.11.1](#)

[Gibraltar 16.10.1](#)

[Micrologiciel programmable sur site \(FPGA\) sur contrôleur LAN sans fil 9800 matériel](#)

[Maintenance logicielle haute disponibilité sur contrôleur LAN sans fil 9800](#)

[ISSU](#)

[Correctif de mise à niveau de maintenance logicielle \(SMU\)](#)

[Ensemble de services pour points d'accès](#)

[Ensemble de périphériques pour points d'accès](#)

[Directives et exigences](#)

[Cisco.com Emplacement des SMU, images APSP et APDP pour différents 9800](#)

[Remarque pour l'accès défini par logiciel \(Software Defined Access ou SDA\)](#)

[Compatibilité IRCM \(Inter-Release Controller Mobility\)](#)

[Pour le code recommandé pour AireOS, reportez-vous à :](#)

[Fonctions prises en charge par les contrôleurs LAN sans fil Catalyst série 9800](#)

Introduction

Ce document décrit comment trouver le logiciel Cisco IOS XE le plus fiable pour les contrôleurs LAN sans fil Catalyst 9800 (WLC C9800).

Fond

Les informations contenues dans ce document s'appliquent à différents facteurs de forme du WLC C9800, notamment :

- Périphériques (9800-40, 9800-80 et 9800-L)
- Contrôleurs virtuels (9800-CL sur les nuages privés et publics)
- Contrôleurs sans fil intégrés sur commutateurs Catalyst série 9000
- Contrôleurs sans fil intégrés sur points d'accès Catalyst (EWC-AP)

Les modèles de point d'accès pris en charge par le C9800 incluent

- Points d'accès 11ac phase 1 basés sur IOS (1700/2700/3700/1572) (pas dans toutes les versions)
- Points d'accès 11ac phase 2 basés sur COS (1800/2800/3800/4800/1540/1560)
- Points d'accès de la gamme Catalyst 11ax 91xx basés sur COS (9105/9115/9117/9120/9130/9136/9164/9166)

La coexistence des WLC AireOS avec le WLC C9800 est prise en compte pour ces recommandations. Les recommandations visent toutes les versions du logiciel Cisco IOS XE applicables aux contrôleurs LAN sans fil Catalyst 9800. En règle générale, une nouvelle version (version de maintenance ou nouvelle séquence de codes) bénéficie d'un temps de stabilisation minimum de 2 à 3 semaines sur le terrain. Si aucun problème grave n'est signalé, elle peut faire

l'objet d'une recommandation générale de Cisco. Ces recommandations sont mises à jour fréquemment à mesure que nous recevons des commentaires par le biais de tests internes, de dossiers TAC, etc.

Versions recommandées par le TAC

IOS XE 17.14.1

La version 17.14.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [notes de version 17.14](#)

Il s'agit de la première version à prendre en charge les WLC CW9800M et CW9800H1/2. Ces WLC peuvent uniquement exécuter des versions postérieures à 17.14.

IOS XE 17.13.1

La version 17.13.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [notes de version 17.13](#)

Dublin 17,12

Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [notes de version 17.12](#). Cisco recommande 17.12.3 pour tous les déploiements. Les sections 17.9.5 et 17.12.3 sont toutes deux recommandées pour le moment.

Voici quelques-uns des principaux avantages de 17.12 par rapport à 17.9 :

- Prise en charge de 6 GHz par davantage de pays
- Possibilité d'utiliser un seul SSID WPA2+WPA3 pour 5 et 6 GHz.
- Algorithme basé sur RRM pour équilibrer la charge des points d'accès sur les processus WNCd

17.12.3

Cisco IOS XE 17.12.3 est la deuxième version de correction de bogue de la catégorie 17.12. Il s'agit de la version recommandée pour tous les déploiements utilisant des fonctionnalités ou du matériel pris en charge dans la version 17.10.1 ou ultérieure.

Si vous avez un déploiement SD-Access, soyez conscient de l'ID de bogue Cisco [CSCwj04031](#)  : WLC force SGT à 0 quand le client libère l'adresse link-local IPv6. Contactez le TAC pour obtenir un correctif SMU si vous êtes concerné.

17.12.2

Cisco IOS XE 17.12.2 est la première version de correction de bogue de la catégorie 17.12 et inclut le correctif pour [CVE-2023-20198 CVE-2023-20273 / CSCwh87343](#). Il s'agit de la version recommandée pour tous les déploiements utilisant des fonctionnalités ou du matériel pris en charge dans la version 17.10.1 ou ultérieure.

Dublin 17.11.1

La version 17.10.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Voir [17.11 EoL Bulletin. Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les Notes de version 17.11.1](#). Pour toutes les fonctionnalités et le matériel pris en charge à partir de 17.10.1 ou 17.11.1, il est recommandé d'utiliser 17.12.2

Dublin 17.10.1

La version 17.10.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Voir [17.10 EoL Bulletin](#). Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [Notes de version 17.10.1](#). Pour toutes les fonctionnalités et le matériel pris en charge à partir de la version 17.10.1, il est recommandé d'utiliser la version 17.12.2

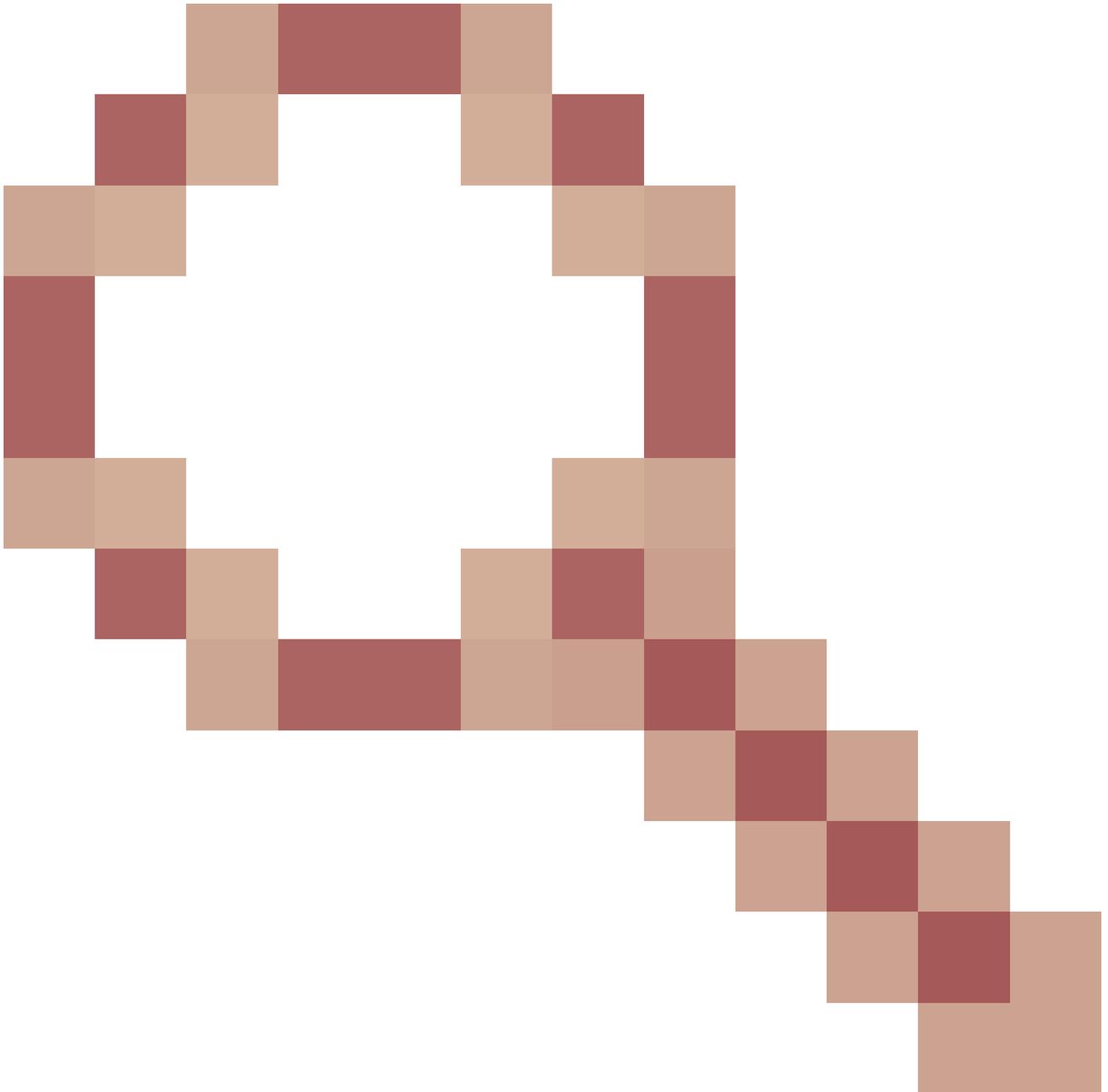
Cupertino 17,9

Cisco IOS XE 17.9.x est un train de longue durée avec plusieurs MR planifiés. [Cisco recommande 17.9.5 pour tous les déploiements.](#)

-
-  Remarque :
- 1) Les PME et les fournisseurs de services avancés requièrent une licence Network Advantage. Pour les déploiements avec une licence Network Essentials, les correctifs de bogues sont disponibles dans l'image de remontée 17.9 qui peut être demandée auprès du TAC Cisco. La mise à niveau vers une image de remontée nécessite un temps d'arrêt.
 - 2) Les PASA sont incrémentielles, c'est-à-dire que chaque version du PASA inclut des correctifs de toutes les versions précédentes des PASA.
 - 3) Évaluez les bogues sous APSP et appliquez les APSP qui incluent des correctifs pour les modèles AP dans votre déploiement.
-

17.9.5

Cisco IOS XE 17.9.5 est une version de correction de bogue, qui corrige tous les problèmes couverts par 17.9.4a ainsi que les APSP. Si vous avez 9162 AP, soyez au courant de [CSCwj45141](#)



qui est un problème qui a commencé dans 17.9.4APSP8

Si vous avez un déploiement SD-Access, soyez conscient de l'ID de bogue Cisco [CSCwj04031](#)  : WLC force SGT à 0 quand le client libère l'adresse link-local IPv6. Contactez le TAC pour obtenir un correctif SMU si vous êtes concerné.

17.9.4 bis

Cisco IOS XE 17.9.4a est publié pour résoudre plusieurs vulnérabilités dans la fonctionnalité d'interface utilisateur Web du logiciel Cisco IOS XE décrite dans [CVE-2023-20198 CVE-2023-20273](#) / [CSCwh87343](#).

Si vous avez un déploiement SD-Access, soyez conscient de l'ID de bogue Cisco [CSCwj04031](#) 

: WLC force SGT à 0 quand le client libère l'adresse link-local IPv6. Contactez le TAC pour obtenir un correctif SMU si vous êtes concerné.

17.9.4a APSP6 (version AP : 17.9.4.201)

17.9.4a APSP6 inclut les mêmes correctifs que 17.9.4 APSP6 même si l'étiquette de version de l'AP est différente de 17.9.4 APSP6. Ces correctifs incluent :

[CSCwh61011 Les](#) points d'accès Cisco 9120 et 9115 se séparent inopinément du WLC et ne peuvent pas établir de nouveau DTLS

[CSCwh7463](#) 3800 n'envoie pas de trames de données QoS en aval en raison de l'indicateur RadarDetected défini sur TRUE

[CSCwh8132](#) 9130AP ont eu des pannes de panique du noyau après la mise à niveau vers 17.6.6 (correctif de régression pour [CSCwf87904](#))

[CSCwh60483](#) 9136I-ROW AP - Mauvaises lectures de température, arrêt de 100s degrés

[CSCwf53520](#) Point d'accès Cisco 1815 exécutant la version 17.9.2 : blocage panique du noyau observé

[CSCwf93992](#) 2800 points d'accès flexibles ne traitent pas les paquets fragmentés EAP-TLS si le délai est supérieur à 50 ms

[CSCwf85025](#) C9166-ROW AP avec code pays GB, réduit txpower après changement de canal causant aux clients de ne pas se connecter.

[CSCwh02913](#) AP plantage du noyau dû à assert:"TXPKTPENDTOT(wlc)== 0" a échoué: fichier "wlc_mutx.c:4247"

[CSCwh08625](#) Panique de noyau sur C9105, C9115, C9120 AP avec PC est à _raw_spin_unlock

[CSCwf68131](#) C9105AXW - contrôle des blocs défectueux

[CSCwf50177](#) C9105AXW - grand nombre de blocs défectueux

17.9.4

Cisco IOS XE 17.9.4 est principalement une version de correction de bogue qui ajoute également

- Assistance Analytique des produits
- Prise en charge de ROW pour UAE

 Mise en garde :

1) Les versions 17.9.4 et 17.9.4a sont affectées par [CSCwf83132](#), ce qui empêche le client de s'associer sur les SSID 11r activés sur les AP flexconnect après un changement de nom de groupe de mobilité.

17.9.4 SMU_CSCwh87343 (SMU à froid ; rechargement requis)

17.9.4 SMU fournit un correctif pour

[CSCwh87343/ CVE-2023-20198 CVE-2023-20273](#) Vulnérabilités multiples dans la fonctionnalité d'interface utilisateur Web du logiciel Cisco IOS XE. Le WLC doit être rechargé pour appliquer ce SMU.

17.9.4 APSP6 (version AP : 17.9.4.206)

17.9.4 APSP5 inclut des correctifs dans APSP1, APSP2 et APSP5 et ajoute également des correctifs pour :

[CSCwh61011 Les](#) points d'accès Cisco 9120 et 9115 se séparent inopinément du WLC et ne peuvent pas établir de nouveau DTLS

[CSCwh7463](#) 3800 n'envoie pas de trames de données QoS en aval en raison de l'indicateur RadarDetected défini sur TRUE

[CSCwh81332](#) 9130AP ont eu des pannes de panique du noyau après la mise à niveau vers 17.6.6 (correctif de régression pour [CSCwf87904](#))

[CSCwh60483](#) 9136I-ROW AP - Mauvaises lectures de température, arrêt de 100s degrés

17.9.4 APSP5 (version AP : 17.9.4.205)

17.9.4 APSP5 inclut des correctifs dans APSP1 et APSP2 et ajoute également des correctifs pour :

[CSCwf53520](#) Point d'accès Cisco 1815 exécutant la version 17.9.2 : blocage panique du noyau observé

[CSCwf93992](#) 2800 points d'accès flexibles ne traitent pas les paquets fragmentés EAP-TLS si le délai est supérieur à 50 ms

17.9.4 APSP2 (version AP : 17.9.4.202)

17.9.4 APSP2 inclut tous les correctifs APSP1 et ajoute également des correctifs pour :

[CSCwf85025](#) C9166-ROW AP avec code pays GB, réduit txpower après changement de canal causant aux clients de ne pas se connecter.

[CSCwh02913](#) AP plantage du noyau dû à assert:"TXPKTPENDTOT(wlc)== 0" a échoué: fichier "wlc_mutx.c:4247"

[CSCwh08625](#) Panique de noyau sur C9105, C9115, C9120 AP avec PC est à _raw_spin_unlock

17.9.4 APSP1 (version AP : 17.9.4.201)

17.9.4 APSP1 fournit des correctifs pour C9105AXW qui adressent :

[CSCwf68131](#) C9105AXW - contrôle des blocs défectueux

[CSCwf50177](#) C9105AXW - grand nombre de blocs défectueux

17.9.3

Cisco IOS XE 17.9.3 est une version de correction de bogue qui ajoute également

- Prise en charge de IW9167E
- Possibilité de spécifier la charge du site pour un meilleur équilibrage de charge des AP sur les instances WNCd (Wireless Network Control Daemon) sur le C9800
- Réintroduit la prise en charge des points d'accès de phase 1 (1700/2700/3700/1572), mais cette prise en charge ne va pas au-delà du cycle de vie normal du produit. Les fonctionnalités de ces points d'accès sont équivalentes à celles de la version 17.3 et la mise à niveau de 17.3.x à 17.9.3 est prise en charge pour $x \geq 4c$. Pour plus de détails, consultez la [FAQ](#)
- Commande pour désactiver la comptabilité AAA provisoire sur le C9800

Si vous exécutez 17.9.3, Cisco recommande, au minimum, d'appliquer des SMU et des APSP et des [ACL HTTP](#) applicables pour [CSCwh87343](#) jusqu'à ce que le WLC puisse être mis à niveau vers 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

17.9.3 + SMU + image CCO APSP4 pour les déploiements avec la gamme AP 11ac phase 2 (2800, 3800, 4800, 1560, 6300) pour répondre à l'[avis de champ FN74035](#) / [CSCwf67316](#)

17.9.3 + SMU + image CCO APSP5 pour les déploiements avec la gamme 11ax Catalyst AP (C9105) pour les adresses [CSCwf68131](#) et [CSCwf50177](#)

17.9.3 + SMU + image CCO APSP3 pour tous les autres déploiements.



Attention : avant de passer à la version 17.9.3,

a. si le WLC C9800 n'exécute pas 17.3.6+APSP6, 17.3.7 ou 17.6.5, alors les AP COS enregistrés sur le WAN vers le WLC risquent de corrompre l'image. Référez-vous à [Comment éviter la boucle de démarrage en raison de la corruption d'image](#) document à la fois pour éviter d'obtenir des AP coincés dans la boucle de démarrage ou pour récupérer des AP coincés dans la boucle de démarrage.

b. Mettez à niveau la version ROMMON sur C9800-40 vers 17.7(3r) pour éviter [CSCvp25150](#) . Reportez-vous à la section FPGA de ce document pour obtenir la version recommandée de ROMMON sur d'autres plates-formes et la procédure de mise à niveau de ROMMON.

17.9.3 SMU

Trois SMU sont publiés pour la version 17.9.3 et incluent des correctifs pour :

[CSCwf5303](#) Le WLC actif redémarre lorsque la liaison RP est activée (sans problème, ne

nécessite pas de rechargement du WLC)

[CSCwe01579](#) plantage WNCd observé à rrm_client_cover_rssi_record_create pendant l'échelle rrm (rechargement du WLC requis)

[CSCwf60151](#) Fuite de mémoire avec blocage de déclenchement pubd sur WLC (sans heurt, ne nécessite pas de rechargement WLC)

17.9.3 APSP5 (Version AP : 17.9.3.205)

17.9.3 APSP4 fournit des correctifs d'AP pour :

[CSCwf68131](#) C9105AXW - contrôle des blocs défectueux

[CSCwf50177](#) C9105AXW - grand nombre de blocs défectueux

17.9.3 APSP4 (Version AP : 17.9.3.204)

17.9.3 APSP3 fournit des correctifs d'AP pour :

[CSCwf67316](#) - 2800/3800/4800/1560/IW6300 ne détecte pas de radar aux niveaux requis

17.9.3 APSP3 (Version AP : 17.9.3.203)

17.9.3 APSP3 fournit des correctifs d'AP pour :

[CSCwe73758](#) Point d'accès 9115 AX Balise bloquée sur 5 GHz

Le périphérique Mac [CSCwf07605](#) C9105AXW et 1815W ne peut pas obtenir d'adresse IP dans le port Ethernet après le remplacement du VLAN AAA

[CSCwe91394](#) Balises Aeroscout T15e ne rapportant pas de données temporaires en raison d'octets supplémentaires après la mise à niveau du WLC vers 17.92 ou 17.10.1

[CSCwf29742](#) FW est tombé en panne lors de l'exécution de la multidiffusion et de la longévité avec plus de 80 clients (après 12 heures)

17.9.3 APSP2 (Version AP : 17.9.3.202)

17.9.2 APSP2 fournit des correctifs d'AP pour :

[CSCwe32853](#) AP C9124AXI ne transmet pas le trafic RLAN au réseau en amont. [SF 06513662]

[CSCwd41463](#) Cisco 3800, 4800 AP cessent d'envoyer un rapport d'adhésion IGMP

17.9.3 APSP1 (Version AP : 17.9.3.201)

17.9.3 APSP1 fournit des correctifs d'AP pour :

[CSCwd91054](#) Lorsque les clients dans le déploiement de l'authentification Flex Central effectuent une itinérance SKC (Sticky Key Caching) avec l'ancien PMKID, ils sont bloqués dans l'état Authentification.

[CSCwe5390](#) 3802AP mise en mémoire tampon UP6/trafic vocal pendant ~500ms après l'itinérance Spectralinkphone entraîne des problèmes audio tels que la voix robotique

[CSCwe04602](#) Le point d'accès COS ne parvient pas à transférer le trafic vers le client sans fil

pendant environ 60 secondes dans les WLAN de fabric SDA

[CSCwe6515](#) 9136 AP dans la version 17.9.2 n'enregistrant pas la réponse M2 du client

[CSCwe8776](#) MAP compatible EWC en attente de 3 minutes en init capwap

17.9.2

Cisco IOS XE 17.9.2 est une version de correction de bogues, à l'exception de quelques nouvelles fonctionnalités (consultez les notes de version pour plus d'informations). Plusieurs corrections de bogues critiques et la prise en charge de versions plus récentes de certains points d'accès WiFi6 Catalyst (reportez-vous à la [notice 72424](#)) sont disponibles dans la version 17.9.2. Il est recommandé de mettre à niveau vers 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

17.9.2 APSP1

17.9.2 APSP1 fournit un correctif pour [CSCwd80290](#) qui permet aux AP IW3700 de rejoindre le WLC C9800 même après le 4 décembre 2022. Pour plus de détails, consultez le site <https://www.cisco.com/c/en/us/support/docs/wireless/aironet-700-series-access-points/218447-ios-ap-image-download-fails-due-to-expir.html> et l'avis de zone [FN72524](#).

17.9.1

Cisco IOS XE 17.9.1 est la première version de la série de versions 17.9.x à longue durée de vie. Il s'agit de la première version à prendre en charge les points d'accès Cisco Catalyst 916x. Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [Notes de version 17.9.1](#). Il est recommandé de mettre à niveau vers 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

 Attention : la prise en charge de versions plus récentes de certains points d'accès WiFi6 Catalyst (reportez-vous à la [notice 72424](#)) n'est **PAS** disponible dans la version 17.9.1, mais dans la version 17.9.2

Cupertino 17.8.1

La version 17.8.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Voir [17.8.1 EoL Bulletin](#). Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [Notes de version 17.8.1](#). Pour toutes les fonctionnalités et le matériel pris en charge à partir de la version 17.8.1, il est recommandé d'utiliser 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

 Remarque : les déploiements avec C9130 et C9124, s'ils exécutent 17.3.3, doivent être mis à niveau vers 17.3.4c avant de passer à 17.8.1

Cupertino 17.7.1

La version 17.7.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Voir [17.7.1 EoL Bulletin](#). Les nouvelles fonctionnalités prises en charge dans cette version sont répertoriées dans les [Notes de version 17.7.1](#). Pour toutes les fonctionnalités et le matériel pris en charge à partir de la version 17.7.1, il est recommandé d'utiliser 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

 Attention : 17.7.1 est affecté par [CSCwb13784](#) qui empêche les AP wave 2 et 11ax de se joindre si le MTU du chemin tombe sous 1000 octets

Bengaluru 17.6

Cisco IOS XE 17.6.x est un train à longue durée de vie avec plusieurs MR. **Il n'y a qu'un seul MR supplémentaire ciblé pour la catégorie 17.6 pour les correctifs de sécurité uniquement.** Reportez-vous au [bulletin 17.6 de fin de vie](#). Cisco vous recommande de migrer vers la version 17.9.5 pour tous les déploiements.

17.6.7

Cisco IOS XE 17.6.7 est une version de correction de bogue uniquement. Il s'agit de la version recommandée si vous devez vous en tenir au train logiciel 17.6.

17.6.6 bis

Cisco IOS XE 17.6.6a corrige [CSCwh87343](#) : Vulnérabilité de remontée des privilèges de l'interface utilisateur Web du logiciel Cisco IOS XE. Il remplace l'article 17.6.6.

17.6.6

Cisco IOS XE 17.6.6 est une version de correction de bogue uniquement.

17.6.5

Cisco IOS XE 17.6.5 est une version de correction de bogue uniquement et ajoute la configuration, sous Policy Profile, pour désactiver la comptabilité provisoire. 17.6.5

17.6.4

Cisco IOS XE 17.6.4 est une version de correction de bogue uniquement et ajoute la configuration, sous AP Join Profile, pour activer la console série AP. Plusieurs corrections de bogues critiques et la prise en charge de versions plus récentes de certains points d'accès WiFi6 Catalyst (reportez-vous à la [notice 72424](#)) sont disponibles dans la version 17.6.4. Cisco recommande de migrer vers 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

17.6.4 APSP1

17.6.4 APSP fournit un correctif pour [CSCwd80290](#) qui permet aux AP IW3700 de rejoindre le WLC C9800 même après le 4 décembre 2022. Pour plus de détails, consultez le site <https://www.cisco.com/c/en/us/support/docs/wireless/aironet-700-series-access-points/218447-ios-ap-image-download-fails-due-to-expir.html> et l'avis de zone [FN72524](#).

17.6.3

La version 17.6.3 de Cisco IOS XE est une version de correction de bogues seulement. Il inclut tous les correctifs dans 17.3.5a + le correctif pour [CSCwb13784](#).

Pour les clients utilisant un emplacement avec des espaces CMX ou DNA, veuillez prendre connaissance de [CSCwb65054](#). SMU (hot patch) publié sur cisco.com.

De nombreux correctifs de bogues fournis via les correctifs SMU dans la version 17.6.3 et la prise en charge de versions plus récentes de certains points d'accès WiFi6 Catalyst (reportez-vous à la [notice 72424](#)) sont disponibles dans la version 17.6.4. Cisco recommande de migrer vers la version 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

17.6.2

Cisco IOS XE 17.6.2 ajoute la prise en charge de quelques fonctionnalités.

- Prise en charge de 802.1 avec échec d'authentification Web sur MAC
- Prise en charge de la technologie Mesh et Mesh + Flex sur les AP extérieurs C9124AXI/E/D
- Limitation bidirectionnelle du débit par client sur les points d'accès Catalyst 802.11ac phase 2 et 11ax

De nombreux bogues critiques sur 17.6.2, par exemple [CSCwb13784](#) qui empêche les AP wave 2 et 11ax de se joindre si le MTU du chemin descend sous 1000 octets, sont résolus dans 17.6.4. Cisco recommande de migrer vers 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

17.6.1

Les nouvelles fonctions prises en charge dans cette version sont indiquées dans les [notes de mise à jour de la version 17.6](#). 17.6.1 est vulnérable à plusieurs défauts critiques et doit être évité.

Bengaluru 17.5.1

La version 17.5.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Reportez-vous au [Bulletin de fin de vie 17.5](#) La liste des fonctionnalités prises en charge dans cette version est répertoriée dans les [Notes de version 17.5](#). Pour tous les nouveaux matériels et fonctionnalités pris en charge à partir de la version 17.5, Cisco vous recommande de migrer vers la version 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

Bengaluru 17.4.1

La version 17.4.1 de Cisco IOS XE est une version de courte durée sans version de maintenance planifiée. Reportez-vous au [bulletin de fin de vie de la version 17.4](#). La liste des fonctions prises en charge dans la version 17.4 est répertoriée dans les [notes de mise à jour de la version 17.4](#). Pour tous les nouveaux matériels et fonctionnalités pris en charge à partir de la version 17.4, Cisco vous recommande de migrer vers la version 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire)

Amsterdam 17.3

Cisco IOS XE 17.3.x est un train à longue durée de vie avec plusieurs versions de maintenance (MR). 17.3 a atteint la fin de la maintenance logicielle, comme indiqué dans le [bulletin de fin de vie 17.3](#). Le dernier MR pour 17.3 est une version Psirt uniquement prévue pour septembre 2023. **Cisco vous recommande de migrer vers la version 17.9.5 pour tous les déploiements si vous utilisez une version antérieure.**

17.3.7

Cisco IOS XE 17.3.7 est le dernier MR de correction de bogue de la version 17.3. Pour les clients qui souhaitent rester dans le train 17.3, Cisco recommande 17.3.7.

17.3.6

Cisco IOS XE 17.3.6 est principalement une version de correction de bogues. Il prend en charge les

- Fonction Mesh et mesh+flex pour les points d'accès 9124 AXI/E/D
- Versions plus récentes (VID) de certains points d'accès WiFi6 Catalyst (reportez-vous à la [notice 7242](#)).

17.3.6 PAA7

APSP7 fournit des correctifs IOS dans APSP5 et des correctifs COS AP dans APSP6 sous forme de correctif unifié.

17.3.6 APSP6 via [CSCwd89180](#)

17.3.6 APSP6 remplace 17.3.6 APSP2 et corrige plusieurs défauts COS AP (11ac wave2 et Catalyst 11ax) :

[CSCvx32806](#) COS-AP bloqués dans la boucle de démarrage en raison d'un échec de vérification de la somme de contrôle de l'image

[CSCwc32182](#) Point d'accès 1852 - Panne de micrologiciel radio (SF 06029787/06121536/06208256)

[CSCwc89719](#) AP1832 Blocage dû à une défaillance radio (échec de la récupération radio) (SF#06180501)

[CSCvz99036](#) Vulnérabilité de contournement VLAN des points d'accès Cisco du VLAN natif

[CSCwd37092](#) Téléchargements TCP lents, échecs d'authentification TLS dans 8.10.181.0/17.3.6 - séries 2800/3800/4800

[CSCwc78435](#) 9130 envoi d'une liste de canaux incorrecte sur un événement DFS hors bande entraînant des problèmes de connectivité client

[CSCwc8148](#) Amélioration supplémentaire pour le problème de suspension mac ([CSCwc72194](#)) côté pilote.

17.3.6 APSP5 via [CSCwd83653](#)

17.3.6 APSP5 fournit un correctif pour l'ID de bogue Cisco [CSCwd80290](#) qui permet aux AP Cisco IOS de rejoindre le WLC C9800 même après le 4 décembre 2022. Pour plus de détails, consultez le site <https://www.cisco.com/c/en/us/support/docs/wireless/aironet-700-series-access-points/218447-ios-ap-image-download-fails-due-to-expir.html> et l'avis de zone [FN72524](#).

17.3.6 APSP2 via [CSCwd40096](#)

17.3.6 APSP2 fournit un correctif pour le bogue Cisco ID [CSCwd37092](#)

Symptôme : téléchargements lents et échecs d'authentification EAP-TLS pour les points d'accès 2800/3800/4800/1560/6300. Pour confirmer le bogue, exécutez `#show controllers nss stats` sur AP et vérifiez si le compteur `INNER_CAPWAP_REASM_FAILED` s'incrémente

Solution : Aucun ; problème de téléchargement TCP uniquement vu sur C9800 lorsque `tcp-adjust-mss 1250` a été explicitement désactivé sous AP Join Profile. L'activation du paramètre empêche les téléchargements TCP lents, mais la lenteur des téléchargements UDP et les échecs EAP-TLS persistent.

Il inclut également le correctif pour l'ID de bogue Cisco [CSCvz99036](#) et l'ID de bogue Cisco [CSCwc78435](#).

17.3.5b

Cisco IOS XE 17.3.5b est une itération mise à jour de 17.3.5a qui intègre des correctifs de bogues fournis via des correctifs SMU et une image d'escalade sur 17.3.5a. Référez-vous [Défauts résolus dans 17.3.5b](#) pour la liste complète.

17.3.5 bis

Cisco IOS XE 17.3.5a contient plusieurs correctifs importants, notamment

- Corrections pour les déclencheurs connus de CPU élevé dans WNCd (sondes, tempête ARP entre autres)
- Priorisation de keepalive CAPWAP pour empêcher les AP de tomber quand l'utilisation du CPU WNCd est à son maximum.
- Syslog pour diagnostiquer le moment où le SSID arrête la diffusion et le mécanisme de récupération CLI. Reportez-vous à [CSCwb01162](#).



Attention : 17.3.5une image CCO est affectée par [CSCwb13784](#) qui empêche les points

 d'accès Wave 2 et 11ax de se joindre si le MTU de chemin descend sous 1000 octets et empêche les points d'accès Cisco IOS (1700/2700/3700) de se joindre si le MTU de chemin descend sous 1500 octets.

Correction : SMU (hot patch) publié sur cisco.com fournit une solution au problème et doit impérativement être appliqué.

17.3.4c

La version 17.3.4c de Cisco IOS XE corrige plusieurs bogues critiques et à grande incidence dans la version 17.3.4.

17.3.4

La version 17.3.4 de Cisco IOS XE est une version de correction de bogues seulement.

 Remarque : les déploiements avec C9130 et C9124, s'ils exécutent 17.3.3, doivent être mis à niveau vers 17.3.4c avant la mise à niveau vers 17.8.1, 17.9.1.

17.3.3

La version 17.3.3 de Cisco IOS XE est une version de correction de bogues seulement.

 Attention : 17.3.3 est vulnérable à [CSCvy11981](#)

Symptôme : panne WNCD

Déclencheur : si un nom d'AP est de 32 caractères ou plus, il y a corruption de mémoire qui conduit à ce crash

Solution : assurez-vous que le nombre de caractères du nom de point d'accès est inférieur ou égal à 31.

17.3.2a

La version 17.3.2a de Cisco IOS XE, bien qu'il s'agisse d'une version de maintenance, ajoute des fonctions en plus des corrections de bogues. Ces fonctions incluent

- Licences Smart à l'aide de la politique [configuration GUI uniquement offerte avec la version 17.4.1]
- OEAP – SSID personnel
- Autorisation de point d'accès à l'aide d'un numéro de série [pour tous les points d'accès sauf ceux qui présentent le certificat wlancc + FIPS + LSC]
- Coexistence de l'assurance et des services IDO sans iCAP
- Tunnel TLS vers DNA-C sur le nuage

17.3.1

Cisco IOS XE 17.3.1 a introduit la prise en charge de ces matériels et solutions

- Points d'accès 9105I et 9105W
- Modèle à débit plus élevé sur 9800CL
- Sans fil intégré sur commutateurs Catalyst 9k (non-SDA)
- Réseau défini par l'utilisateur (UDN) et application mobile UDN
- Gestion BLE sur le contrôleur
- Gestion du module IDO

Pour consulter la liste complète, reportez-vous [aux notes de mise à jour de la version 17.3.](#)

Amsterdam 17.2.1

La version 17.2.1 de Cisco IOS XE est une série de courte durée sans version de maintenance planifiée. Reportez-vous au [bulletin de fin de vie de la version 17.2](#). Toutes les versions 17.2.x de C9800 sont reportées en raison de l'[avis publié FN70577](#) et de [CSCvu24770](#). Cisco recommande la migration vers la version 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire) pour tous les déploiements.

Amsterdam 17.1.1

La version 17.1.1 de Cisco IOS XE est une version de courte durée sans maintenance planifiée. Reportez-vous au [bulletin de fin de vie de la version 17.1](#). Toutes les versions 17.2.x de C9800 sont reportées en raison de l'[avis publié FN70577](#) et de [CSCvu24770](#). Cisco recommande la migration vers la version 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire) pour tous les déploiements.

Gibraltar 16.12

Cisco IOS XE 16.12 est la première version longue durée du 9800. La version 16.12.1 a introduit la prise en charge de ces matériels et solutions.

- 9800-L
- 9800-CL sur Google Cloud
- 9120AXE, 9130AXI
- Contrôleur sans fil intégré sur point d'accès Catalyst (EWC-AP)

16.12.8

Toutes les versions 16.12.x de 16.12.2 à 16.12.7 sont des versions correctrices de bogues uniquement. 16.12.8 est le dernier MR prévu dans ce train. Reportez-vous au [bulletin de fin de vie de la version 16.12](#). Cisco vous recommande de migrer vers la version 17.9.5 pour tous les déploiements.



Remarque : toutes les versions de 16.12.x antérieures à 16.12.4a (16.12.1, 16.12.1s, 16.12.1t, 16.12.2s, 16.12.2t, 16.12.3, 16.12.3s) sont reportées à l'adresse [CSCvu24770](#).

Gibraltar 16.11.1

La version 16.11.1 de Cisco IOS XE est une version de courte durée sans autre maintenance planifiée. Reportez-vous au [bulletin de fin de vie](#). Pour toutes les fonctionnalités de la version 16.x, Cisco recommande la migration vers la version 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire) pour tous les déploiements

Gibraltar 16.10.1

Cisco IOS XE 16.10.1 est la première version du logiciel Cisco IOS XE qui prend officiellement en charge les références Catalyst 9800 (appliances : 9800-40, 9800-80 ; 9800 sur le cloud privé/public ; 9800-CL, ainsi que le logiciel 9800 sur les commutateurs Catalyst 9300). La version 16.10.1e de Cisco IOS XE est la première à prendre en charge l'intégration de Cisco DNA Center avec le Catalyst 9800. Il s'agit d'une version de courte durée sans aucune version de maintenance (MR) planifiée. Reportez-vous au bulletin de fin de vie. Pour toutes les fonctionnalités de la version 16.x, Cisco recommande la migration vers 17.9.4 + SMU_CSCwh87343 + APSP (si nécessaire) OU 17.9.4a + APSP (si nécessaire) pour tous les déploiements.

Micrologiciel programmable sur site (FPGA) sur contrôleur LAN sans fil 9800 matériel

Sur les contrôleurs LAN sans fil Catalyst 9800 physiques (9800L, 9800-40 et 9800-80), en plus d'IOS-XE, deux autres éléments de code peuvent être mis à niveau.

- Moniteur ROM (ROMMON) : Il s'agit du programme de démarrage qui initialise le matériel et démarre le logiciel IOS-XE sur l'appareil C9800. Vous pouvez vérifier la version de ROMMON de votre appareil en exécutant la commande ci-dessous.

```
#show rom-monitor chassis {active | standby} R0
```

- PHY : Il s'agit de la couche physique, en particulier du module de l'adaptateur de port partagé (SPA), qui prend en charge la distribution frontale et les ports de liaison ascendante sur les appareils C9800. Vous pouvez afficher la version PHY de votre appareil en exécutant la commande ci-dessous.

```
#show platform hardware chassis active qfp datapath pmd ifdev | include FW
```

Un nouveau micrologiciel est généralement publié pour protéger l'intégrité du système (capteurs de température, ventilateur, alimentation, etc.) et pour résoudre les problèmes de transfert de données à l'intérieur et à l'extérieur des ports physiques. [Cisco recommande la mise à niveau vers le dernier micrologiciel FPGA disponible](#). Procédure de mise à niveau ainsi que les défauts pour lesquels un nouveau micrologiciel a été lancé, s'ils sont documentés lors de la mise à niveau du FPGA C9800. Le tableau 1 dresse la liste des versions pour chaque plateforme.

	ROMMON	PHY Ethernet	PHY fibre optique
9800-L-F	16.12(3r)	S/O	17.11.1
9800-L-C	16.12(3r)	17.11.1	S/O
9800-40	17.7(3r)	S/O	16.0.0
9800-80	17.3(3r)	S/O	16.0.0

Maintenance logicielle haute disponibilité sur contrôleur LAN sans fil 9800

Le C9800 offre plusieurs fonctions qui assurent la disponibilité pendant la phase de maintenance logicielle du cycle de vie du déploiement. Il s'agit notamment de la mise à niveau logicielle en service (ISSU), de la mise à niveau progressive des points d'accès, des correctifs à chaud et à froid pour traiter les défauts ou les PSIRT du contrôleur LAN sans fil, des correctifs pour traiter certains problèmes propres aux points d'accès ainsi que pour prendre en charge les nouveaux modèles de points d'accès sur le code de contrôleur existant.

ISSU

La prise en charge d'ISSU a été ajoutée dans la version 17.3.1 et se limite aux versions de longue durée (17.3.x, 17.6.x et 17.9.x). Autrement dit, l'ISSU fonctionne :

1. Dans les versions majeures de longue durée, par exemple, 17.3.x à 17.3.y, 17.6.x à 17.6.y et 17.9.x à 17.9.y
2. Entre les versions majeures de longue durée, par exemple, 17.3.x à 17.6.x et 17.3.x à 17.9.x

Remarque : cette option est limitée à deux versions à longue durée de vie après la version à longue durée de vie actuellement prise en charge.

L'ISSU n'est PAS prise en charge :

1. Dans les versions mineures de séries de versions de courte durée, par exemple 17.4.x à 17.4.y ou 17.5.x à 17.5.y
2. Entre les versions mineures et majeures des séries de versions de courte durée, par exemple 17.4.x à 17.5.x
3. Entre les versions de longue durée et de courte durée 17.3.x à 17.4.x ou 17.5.x à 17.6.x.

Correctif de mise à niveau de maintenance logicielle (SMU)

Le C9800 prend en charge les correctifs à froid et à chaud, ce qui permet de fournir des corrections de bogues sous forme de fichier de mise à niveau de maintenance logicielle (SMU).

- Correctif à chaud : Le rechargement du système n'est pas nécessaire, ce qui signifie que le contrôleur LAN sans fil et les points d'accès continuent de fonctionner. Dans le cas d'une paire de basculement dynamique (SSO) 9800, le processus d'installation de la SMU applique le correctif aux deux châssis.

- Correctif à froid : Un rechargement du système est nécessaire pour un correctif à froid. Dans le cas d'une paire SSO 9800, le correctif à froid peut être appliqué sans temps d'arrêt.

Ensemble de services pour points d'accès

Les correctifs pour les défauts logiciels sur les points d'accès (AP) peuvent être fournis par l'intermédiaire d'ensembles de services pour points d'accès. Cette méthode nécessite le rechargement des points d'accès, mais pas du contrôleur LAN sans fil 9800.

Ensemble de périphériques pour points d'accès

La prise en charge des nouveaux modèles de points d'accès est possible sur le code du contrôleur LAN sans fil existant, sans qu'il soit nécessaire de mettre à niveau ce code. Ce point d'accès prend uniquement en charge les fonctionnalités disponibles dans le code WLC existant.

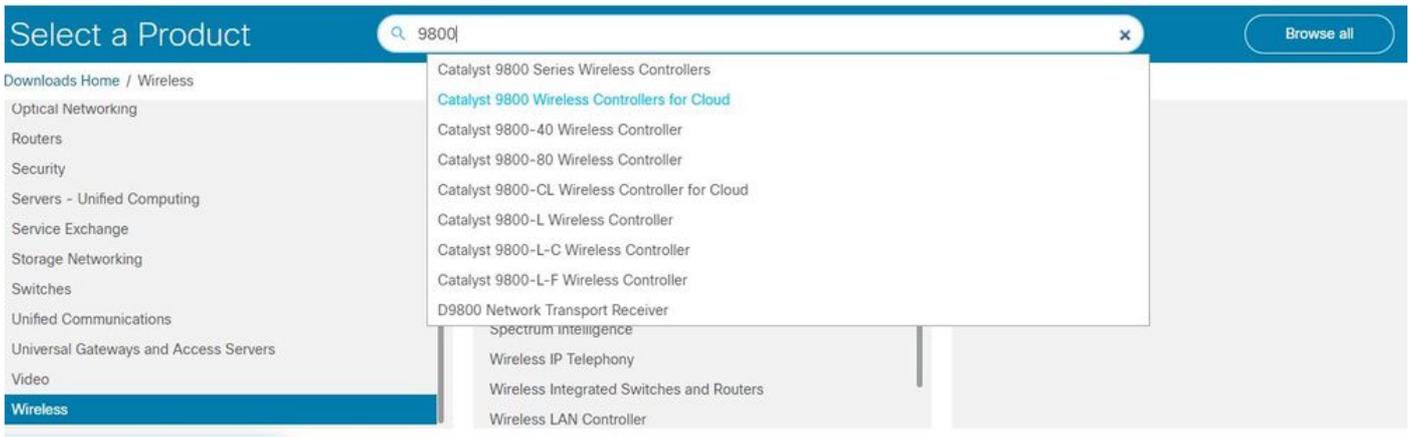
Directives et exigences

1. Les correctifs SMU ne sont générés que pour les versions à longue durée de vie telles que 16.12, 17.3, 17.6, 17.9 et ainsi de suite après leur version MD.
2. Les SMU peuvent seulement être appliquées aux contrôleurs LAN sans fil 9800 exécutant au minimum la licence Network Advantage. Reportez-vous au [tableau des fonctions sans fil pour connaître les différentes licences.](#)
3. Les SMU applicables à la plupart des déploiements sont publiées sur cisco.com pour que les clients puissent les télécharger eux-mêmes.
4. Des SMU ou des correctifs ne sont pas offerts pour toutes les corrections de bogues. Les modifications de code en cause dans la correction de bogues déterminent généralement la possibilité d'appliquer des correctifs.
5. L'applicabilité de la SMU est évaluée pour chaque défaut. Si votre C9800 est admissible à un correctif SMU, en fonction de sa licence et que vous avez besoin d'un correctif SMU pour un défaut spécifique, contactez le centre d'assistance technique Cisco (TAC) pour obtenir l'évaluation du bogue.

Reportez-vous au [guide des correctifs du contrôleur LAN sans fil C9800](#) pour en savoir plus sur ces fonctions.

Cisco.com Emplacement des SMU, images APSP et APDP pour différents 9800

Étape 1. Rendez-vous à l'accueil des téléchargements [et](#) entrez 9800 dans la barre de recherche pour sélectionner un produit, puis choisissez le format de périphérique 9800 applicable.



Étape 2. Dans le menu Software Type (type de logiciel), sélectionnez SMU, APSP ou APDP, selon vos besoins.

Select a Software Type

IOS XE Hardware Programmable Devices

IOS XE In-Service Software Upgrade (ISSU) Matrix

IOS XE ROMMON Software

IOS XE Software

IOS XE Software AP Device Pack

IOS XE Software AP Service Pack

IOS XE Software Maintenance Upgrades (SMU)

Management Information Base (MIB)

NBAR2 Protocol Packs

Wireless Lan Controller Web Authentication Bundle

Remarque pour l'accès défini par logiciel (Software Defined Access ou SDA)

Reportez-vous toujours à la [matrice de compatibilité SDA](#) pour connaître les recommandations de combinaisons de codes optimales pour le SDA. Elle répertorie les combinaisons données de codes sur Cisco DNA Center, le moteur du service de vérification des identités (ISE), les commutateurs, les routeurs et les codes de contrôleur LAN sans fil qui ont été testés par l'équipe de test de solutions SDA de Cisco.

Compatibilité IRCM (Inter-Release Controller Mobility)

- IRCM n'est pas pris en charge avec les contrôleurs 2504/7510/vWLC et est uniquement pris en charge avec les plates-formes 5508/8510/5520/8540/3504.
- Pour la compatibilité de la mobilité du contrôleur entre les versions (IRCM) avec les WLC AireOS,
 - Le TAC recommande AireOS 8.10.190.0 pour tous les déploiements.
 - Pour les déploiements avec des WLC ou des points d'accès plus anciens dans leur environnement, qui ne peuvent pas être mis à niveau après AireOS 8.5, le TAC recommande [8.5.182.108 \(post caché\)](#) code IRCM.

Remarque : toutes les versions du code 8.5 ne prennent pas en charge IRCM. Les versions 8.5 d'IRCM disponibles sur cisco.com incluent 8.5.164.0, 8.5.164.216, 8.5.176.0, 8.5.176.1, 8.5.176.2 et 8.5.182.104.

Pour le code recommandé pour AireOS, reportez-vous à :

<https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/200046-tac-recommended-airios.html>

Fonctions prises en charge par les contrôleurs LAN sans fil Catalyst série 9800

[notes de version](#)

[Liste des fonctions sans fil de Cisco IOS XE par version](#)

[Tableau de comparaison des fonctions d'AireOS à Cisco IOS XE](#)

[Tableau des fonctions Flexconnect pour les points d'accès Wave2 et 11ax](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.