

Release consigliate di Cisco IOS XE per i dispositivi Catalyst 9800 Wireless LAN Controller

Sommario

[Introduzione](#)

[Introduzione](#)

[Build consigliate dal centro TAC](#)

[IOS XE 17.15](#)

[17.15.1](#)

[IOS XE 17.14.1](#)

[IOS XE 17.13.1](#)

[Dublino 17.12](#)

[17.12.4](#)

[17.12.3](#)

[17.12.2](#)

[Dublino 17.11.1](#)

[Dublino 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](#)

[17.3.5 ter](#)

[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](#)

[Firmware programmabile sul campo \(FPGA\) sui WLC 9800](#)

[Manutenzione del software High Availability sui WLC 9800](#)

[ISSU](#)

[Patch SMU \(Software Maintenance Upgrade\)](#)

[Service Pack per access point](#)

[Device Pack per access point](#)

[Linee guida e requisiti](#)

[Ubicazione delle immagini SMU, APSP e APDP per i vari controller 9800 sul sito cisco.com](#)

[Nota per Software Defined Access \(SDA\)](#)

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

[Per il software AireOS consigliato, fare riferimento a:](#)

[Funzionalità supportate sui Catalyst serie 9800 Wireless LAN Controller](#)

Introduzione

In questo documento viene descritto come trovare il software Cisco IOS XE più affidabile per i controller Catalyst 9800 Wireless LAN (C9800 WLC).

Introduzione

Le informazioni di questo documento si applicano a diversi fattori di forma del WLC C9800, tra cui:

- Appliance (9800-40, 9800-80, 9800-L)
- Virtual Controller (9800-CL in cloud pubblici e privati)
- Embedded Wireless Controller sugli switch Catalyst serie 9000
- Embedded Wireless Controller sugli access point Catalyst (EWC-AP)

I modelli di Access Point supportati da C9800 includono

- Access point 11ac Wave 1 basato su IOS (1700/2700/3700/1572) (non in tutte le versioni)
- Access point 11ac Wave 2 basato su COS (1800/2800/3800/4800/1540/1560)
- Access point Catalyst serie 11ax 91xx basato su COS (9105/9115/9117/9120/9130/9136/9164/9166)

Per queste raccomandazioni si tiene conto della coesistenza dei WLC di AireOS con i WLC del C9800. Le raccomandazioni riguardano tutte le release del software Cisco IOS XE applicabili ai WLC Catalyst 9800. In genere, a una versione appena rilasciata (versione di manutenzione o nuovo code train) viene assegnato un tempo di immersione minimo di 2-3 settimane nel campo e, solo se non vengono segnalati problemi catastrofici, diventa un candidato per le raccomandazioni

generali di Cisco. Queste raccomandazioni vengono aggiornate di frequente in seguito a test interni, casi TAC e così via.

Build consigliate dal centro TAC

IOS XE 17.15

IOS XE 17.15 è un treno di lunga durata con diverse versioni di manutenzione (MR) in programma.

17.15.1

IOS XE 17.15.1 è la prima versione del treno 17.15. Questa è la versione consigliata se si usano i nuovi WLC CW9800H o CW9800M che possono eseguire solo versioni successive alla 17.14

17.15.1 contiene la correzione per la vulnerabilità "regreSSHion" sui punti di accesso rappresentati nell'ID bug Cisco [CSCwk62269](#)

IOS XE 17.14.1

Cisco IOS XE 17.14.1 è una release di breve durata senza release di manutenzione pianificate. Le nuove funzionalità supportate in questa release sono elencate nelle [note sulla release 17.14](#)

Questa è la prima versione a supportare i WLC CW9800M e CW9800H1/2. Tali WLC possono eseguire solo versioni successive alla 17.14.

IOS XE 17.13.1

Cisco IOS XE 17.13.1 è una release di breve durata senza release di manutenzione pianificate. Le nuove funzionalità supportate in questa release sono elencate nelle [note sulla release 17.13](#)

Dublino 17.12

Le nuove funzionalità supportate in questa release sono elencate nelle [note sulla release 17.12](#). Cisco consiglia 17.12.3 per tutte le implementazioni. Si consiglia di utilizzare sia la versione 17.9.5 che la versione 17.12.3.

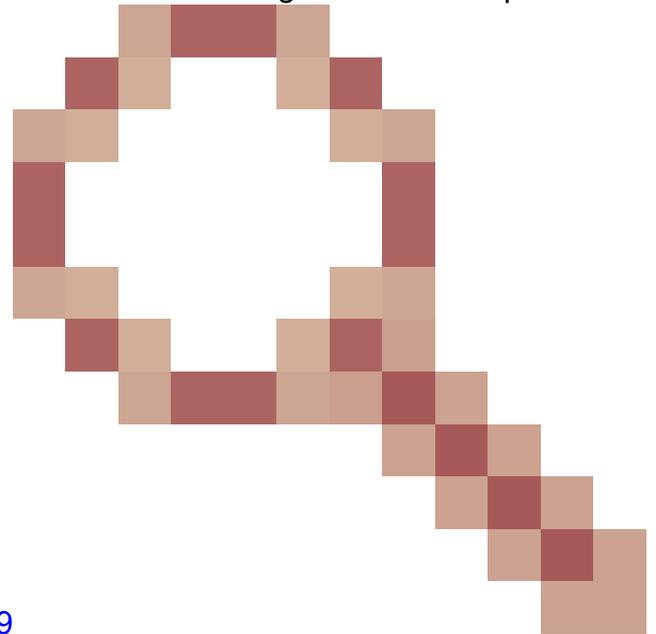
Tra i principali vantaggi di 17,12 rispetto a 17,9 vi sono:

- Supporto di più paesi per 6 GHz
- Possibilità di utilizzare un singolo SSID WPA2+WPA3 per 5 e 6 GHz.
- Algoritmo basato su RRM per bilanciare il carico degli access point tra i processi WNCd

17.12.4

Cisco IOS XE 17.12.4 è la terza versione in cui è stato risolto il problema di bug nel treno della versione 17.12. Non è ancora la release consigliata per la versione 17.12, ma è attualmente in

fase di valutazione. 17.12.4 contiene la correzione per la vulnerabilità "regreSSHion" sui punti di



accesso rappresentati nell'ID bug Cisco [CSCwk62269](#)

17.12.3

Cisco IOS XE 17.12.3 è la seconda versione per la correzione di bug del treno 17.12. Questa è la versione consigliata per tutte le distribuzioni che utilizzano le funzionalità o l'hardware supportato nella versione 17.10.1 o successive.

Se si dispone di un'implementazione SD-Access, tenere presente l'ID bug Cisco [CSCwj04031](#)  : il WLC forza il valore SGT su 0 quando il client rilascia l'indirizzo locale del collegamento IPv6. Se il problema persiste, contattare TAC per ottenere una patch SMU.

17.12.2

Cisco IOS XE 17.12.2 è la prima versione per la correzione di bug del treno 17.12 e include la correzione per [CVE-2023-20198 CVE-2023-20273 / CSCwh87343](#). Questa è la versione consigliata per tutte le distribuzioni che utilizzano le funzionalità o l'hardware supportato nella versione 17.10.1 o successive.

Dublino 17.11.1

Cisco IOS XE 17.10.1 è una release di breve durata senza release di manutenzione pianificate. Cfr. [17.11 Bollettino EoL](#). Le nuove funzionalità supportate in questa release sono elencate nelle [note sulla release 17.11.1](#). Per tutte le funzionalità e i componenti hardware supportati a partire dalla versione 17.10.1 o 17.11.1, si consiglia di utilizzare la versione 17.12.2

Dublino 17.10.1

Cisco IOS XE 17.10.1 è una release di breve durata senza release di manutenzione pianificate. Vedere [17.10 EoL Bulletin](#). Le nuove funzionalità supportate in questa release sono elencate nelle

[note sulla release 17.10.1](#). Per tutte le funzionalità e i componenti hardware supportati a partire dalla versione 17.10.1, si consiglia di utilizzare la versione 17.12.2

Cupertino 17.9

Cisco IOS XE 17.9.x è un treno che ha una vita lunga e che ha in programma diversi MR. [Cisco consiglia 17.9.5 per tutte le implementazioni. Si consiglia di utilizzare sia la versione 17.9.5 che la versione 17.12.3.](#)

Nota:

- 1) SMU e APSP richiedono una licenza Network Advantage. Per le implementazioni con licenza Network Essentials, le correzioni dei bug sono disponibili nell'immagine 17.9 Escalation, che può essere richiesta a Cisco TAC. L'aggiornamento a un'immagine Escalation richiede tempi di inattività.
- 2) Gli APSP sono incrementali, ovvero ogni versione di APSP include correzioni da tutte le versioni precedenti di APSP.
- 3) Valutare i bug in APSP e applicare gli APSP che includono le correzioni per i modelli AP nella propria implementazione.

17.9.5

Cisco IOS XE 17.9.5 è una versione per la correzione di tutti i problemi risolti dalla versione

17.9.4a e dagli APSP. Se si dispone di 9162 AP, tenere presente che [CSCwj45141](#) è un problema iniziato nella versione 17.9.4APSP8

Se si dispone di un'implementazione SD-Access, tenere presente l'ID bug Cisco [CSCwj04031](#)  : il WLC forza il valore SGT su 0 quando il client rilascia l'indirizzo locale del collegamento IPv6. Se il problema persiste, contattare TAC per ottenere una patch SMU.

17.9.4 bis

Cisco IOS XE 17.9.4a viene pubblicato per risolvere diverse vulnerabilità nella funzionalità UI Web del software Cisco IOS XE descritta in [CVE-2023-20198](#) [CVE-2023-20273](#) / [CSCwh87343](#).

Se si dispone di un'implementazione SD-Access, tenere presente l'ID bug Cisco [CSCwj04031](#)  : il WLC forza il valore SGT su 0 quando il client rilascia l'indirizzo locale del collegamento IPv6. Se il problema persiste, contattare TAC per ottenere una patch SMU.

17.9.4a APSP6 (versione AP: 17.9.4.201)

17.9.4a APSP6 include le stesse correzioni della versione 17.9.4 APSP6 anche se l'etichetta della versione AP è diversa da 17.9.4 APSP6. Queste correzioni includono:

[CSCwh61011](#) Cisco 9120 e 9115 AP: separazioni impreviste dal WLC e impossibile stabilire nuovamente DTLS

[CSCwh7463](#) 3800: impossibile inviare i frame dati QoS a valle a causa del flag RadarDetected come TRUE

[CSCwh8132](#) 9130AP ha riportato un arresto anomalo del kernel dopo l'aggiornamento alla versione 17.6.6 (correzione rapida per [CSCwf87904](#))

[CSCwh60483](#) 9136I-ROW AP - Letture della temperatura errate, disattivate di 100 gradi

[CSCwf53520](#) Cisco 1815 AP con versione 17.9.2: Rilevato arresto anomalo del kernel

[CSCwf9392](#) 2800 Flex AP non elabora i pacchetti frammentati EAP-TLS se il ritardo è superiore a 50 ms

[CSCwf85025](#) C9166-ROW AP con codice paese GB, riduce la potenza di trasmissione dopo il cambio di canale, che impedisce ai client di connettersi.

Arresto anomalo del kernel [CSCwh02913](#) AP dovuto a asserzione: "TXPKTPENDTOT(wlc)== 0" non riuscito: file "wlc_mutx.c:4247"

[CSCwh08625](#) Errore kernel su C9105, C9115, C9120 AP con PC in _raw_spin_unlock

[CSCwf68131](#) C9105AXW - monitoraggio blocco danneggiato

[CSCwf50177](#) C9105AXW - numero elevato di blocchi danneggiati

17.9.4

Cisco IOS XE 17.9.4 è principalmente una versione per la correzione di bug che aggiunge

- Supporto dell'analisi dei prodotti
- Supporto ROW per EAU



Attenzione:

1) Le versioni 17.9.4 e 17.9.4a sono interessate da [CSCwf83132](#), che impedisce l'associazione del client agli SSID abilitati per 11r sugli access point flexconnect dopo la modifica del nome di un gruppo di mobilità.

17.9.4 SMU_CSCwh87343 (SMU a freddo; richiede il ricaricamento)

17.9.4 SMU fornisce la correzione per

[CSCwh87343](#)/ [CVE-2023-20198](#) [CVE-2023-20273](#) Multiple Vulnerability in Cisco IOS XE Software Web UI Feature. Il WLC deve essere ricaricato per applicare questa SMU.

17.9.4 APSP6 (versione AP: 17.9.4.206)

17.9.4 APSP5 include correzioni in APSP1, APSP2 e APSP5 e inoltre aggiunge correzioni per:

[CSCwh61011](#) Cisco 9120 e 9115 AP: separazioni impreviste dal WLC e impossibile stabilire nuovamente DTLS

[CSCwh7463](#) 3800: impossibile inviare i frame dati QoS a valle a causa del flag RadarDetected come TRUE

[CSCwh8132](#) 9130AP ha riportato un arresto anomalo del kernel dopo l'aggiornamento alla versione 17.6.6 (correzione rapida per [CSCwf87904](#))

[CSCwh60483](#) 9136I-ROW AP - Letture della temperatura errate, disattivate di 100 gradi

17.9.4 APSP5 (versione AP: 17.9.4.205)

17.9.4 APSP5 include correzioni in APSP1 e APSP2 e aggiunge correzioni per:

[CSCwf53520](#) Cisco 1815 AP con versione 17.9.2: Rilevato arresto anomalo del kernel

[CSCwf9392](#) 2800 Flex AP non elabora i pacchetti frammentati EAP-TLS se il ritardo è superiore a 50 ms

17.9.4 APSP2 (versione AP: 17.9.4.202)

17.9.4 APSP2 include tutte le correzioni APSP1 e aggiunge correzioni per:

[CSCwf85025](#) C9166-ROW AP con codice paese GB, riduce la potenza di trasmissione dopo il cambio di canale, che impedisce ai client di connettersi.

Arresto anomalo del kernel [CSCwh02913](#) AP dovuto a asserzione: "TXPKTPENDTOT(wlc)== 0" non riuscito: file "wlc_mutx.c:4247"

[CSCwh08625](#) Errore kernel su C9105, C9115, C9120 AP con PC in _raw_spin_unlock

17.9.4 APSP1 (versione AP: 17.9.4.201)

17.9.4 APSP1 fornisce le correzioni per C9105AXW relative a:

[CSCwf68131](#) C9105AXW - monitoraggio blocco danneggiato

[CSCwf50177](#) C9105AXW - numero elevato di blocchi danneggiati

.

17.9.3

Cisco IOS XE 17.9.3 è una versione per la correzione dei bug che aggiunge

- Supporto per IW9167E
- Possibilità di specificare il carico del sito per un migliore bilanciamento del carico dei punti di accesso tra le istanze WNC (Wireless Network Control Daemon) sul server C9800
- Reintroduce il supporto per i punti di accesso Wave 1 (1700/2700/3700/1572), ma questo supporto non va al di là del normale supporto del ciclo di vita del prodotto. Le funzionalità di

questi access point sono uguali a quelle della versione 17.3, mentre l'aggiornamento dalla versione 17.3.x alla 17.9.3 è supportato per x >=4c. Per ulteriori informazioni, vedere le [domande frequenti](#)

- Comando per disabilitare AAA Interim Accounting su C9800

Se la versione 17.9.3 è in esecuzione, Cisco consiglia, come minimo, di applicare le SMU, le APSP e gli [ACL HTTP](#) applicabili per [CSCwh87343](#) finché il WLC non può essere aggiornato alla versione 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O alla versione 17.9.4a + APSP (in base alle esigenze)

17.9.3 + SMU + immagine CCO APSP4 per installazioni con 11ac wave serie 2 AP (2800, 3800, 4800, 1560, 6300) per rispondere all'[avviso sul campo FN74035](#) / [CSCwf67316](#)

17.9.3 + SMU + immagine CCO APSP5 per implementazioni con 11ax Catalyst serie AP (C9105) per indirizzare a [CSCwf68131](#) e [CSCwf50177](#)

17.9.3 + SMU + immagine CCO APSP3 per tutte le altre implementazioni.

-
-  **Attenzione:** prima di eseguire l'aggiornamento a 17.9.3,
- a. se il WLC C9800 non è in esecuzione alla versione 17.3.6+APSP6, 17.3.7 o 17.6.5, gli AP COS registrati sulla WAN sul WLC sono a rischio di danneggiamento dell'immagine. Per [evitare che i punti di accesso siano bloccati nel loop di avvio o per ripristinare i punti di accesso bloccati nel loop di avvio, consultare il](#) documento sulla [prevenzione del loop di avvio a causa di un danneggiamento dell'immagine](#).
 - b. Aggiornare la versione di ROMMON su C9800-40 alla versione 17.7(3r) per evitare l'uso di [CSCvp25150](#) . Fare riferimento alla sezione FPGA di questo documento per la versione consigliata di ROMMON su altre piattaforme e la procedura di aggiornamento di ROMMON.
-

17.9.3 PMI

Nella versione 17.9.3 vengono pubblicate tre SMU che includono correzioni per:

[CSCwf5303](#) Active WLC si riavvia quando arriva il collegamento RP (hitless, non richiede il ricaricamento WLC)

[CSCwe01579](#) WNCd crash osservato in rm_client_coverage_rssi_record_create durante la scalabilità rm (richiede il ricaricamento del WLC)

[CSCwf60151](#) Perdita di memoria con arresto anomalo del server sul WLC (hitless, non richiede il ricaricamento del WLC)

17.9.3 APSP5 (versione AP: 17.9.3.205)

17.9.3 APSP4 fornisce correzioni AP per:

[CSCwf68131](#) C9105AXW - monitoraggio blocco danneggiato

[CSCwf50177](#) C9105AXW - numero elevato di blocchi danneggiati

17.9.3 APSP4 (versione AP: 17.9.3.204)

17.9.3 APSP3 fornisce correzioni AP per:

[CSCwf67316](#) - 2800/3800/4800/1560/IW6300 non è in grado di rilevare il radar sui livelli richiesti

17.9.3 APSP3 (versione AP: 17.9.3.203)

17.9.3 APSP3 fornisce correzioni AP per:

[CSCwe73758](#) 9115 AX AP Beacon bloccato su 5 GHz

[CSCwf07605](#) C9105AXW e 1815W Mac non riescono a ottenere un indirizzo IP nella porta Ethernet dopo l'override della VLAN AAA

[CSCwe91394](#) Aeroscout T15e Tag che non segnalano dati temporanei a causa di byte extra dopo l'aggiornamento di WLC a 17.9.2 o 17.10.1

[CSCwf29742](#) FW si è bloccato durante l'esecuzione di Multicast e Longevità con oltre 80 client (dopo 12 ore)

17.9.3 APSP2 (versione AP: 17.9.3.202)

17.9.2 APSP2 fornisce correzioni AP per:

[CSCwe32853](#) AP C9124AXI non inoltra il traffico RLAN alla rete a monte. [SF 06513662]

[CSCwd41463](#) Cisco 3800, 4800 AP: interruzione dell'invio del rapporto di appartenenza IGMP

17.9.3 APSP1 (versione AP: 17.9.3.201)

17.9.3 APSP1 fornisce correzioni AP per:

[CSCwd91054](#) Quando i client nella distribuzione dell'autenticazione centrale Flex eseguono il roaming con il vecchio PMKID utilizzando la funzionalità di memorizzazione nella cache permanente (SKC), rimangono bloccati nello stato di autenticazione.

[CSCwe55390](#) 3802AP buffering UP6/traffico vocale per circa 500 ms dopo il roaming del telefono Spectralink causa problemi audio come la voce robotica

[CSCwe04602](#) COS AP non riesce a inoltrare il traffico al client wireless per circa 60 secondi nelle WLAN del fabric SDA

[CSCwe6515](#) 9136 AP nella versione 17.9.2 senza registrazione della risposta M2 del client

[CSCwe88776](#) EWC compatibile MAP in attesa di 3 minuti in capwap init

17.9.2

Cisco IOS XE 17.9.2 è una versione per la correzione di bug, ad eccezione di un paio di nuove funzionalità (per ulteriori informazioni, vedere le note sulla versione). Diverse correzioni di bug critici e il supporto per le versioni più recenti di alcuni punti di accesso Catalyst WiFi6 (fare riferimento alla [notifica sul campo 72424](#)) sono disponibili nella versione 17.9.2. Si consiglia di eseguire l'aggiornamento a 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O 17.9.4a + APSP (in base alle esigenze)

17.9.2 PSP1

17.9.2 APSP1 fornisce una correzione per [CSCwd80290](#) che consente agli IW3700 AP di collegarsi al WLC anche dopo il 4 dicembre 2022. Per ulteriori informazioni, consultare il sito <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> e la notifica sul campo FN72524.

17.9.1

Cisco IOS XE 17.9.1 è la prima versione del longevo 17.9.x release train. Questa è la prima versione a supportare i Cisco Catalyst serie 916x AP. Le nuove funzionalità supportate in questa release sono elencate nelle [Note sulla release 17.9.1](#). Si consiglia di eseguire l'aggiornamento a 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O 17.9.4a + APSP (in base alle esigenze)

 Attenzione: il supporto per le versioni più recenti di alcuni Access Point Catalyst WiFi6 (fare riferimento alla [Notifica 72424](#)) **NON** è disponibile nella versione 17.9.1, ma è presente nella versione 17.9.2

Cupertino 17.8.1

Cisco IOS XE 17.8.1 è una release di breve durata senza release di manutenzione pianificate. Cfr. [17.8.1 Bollettino EoL](#). Le nuove funzionalità supportate in questa release sono elencate nelle [note sulla release 17.8.1](#). Per tutte le funzionalità e i componenti hardware supportati a partire dalla versione 17.8.1, si consiglia di utilizzare 17.9.4 + SMU_CSCwh87343 + APSP (se necessario) O 17.9.4a + APSP (se necessario)

 Nota: le distribuzioni con C9130 e C9124s, se si utilizza la versione 17.3.3, devono essere aggiornate alla versione 17.3.4c prima dell'aggiornamento alla versione 17.8.1

Cupertino 17.7.1

Cisco IOS XE 17.7.1 è una release di breve durata senza release di manutenzione pianificate. Cfr. [17.7.1 Bollettino EoL](#). Le nuove funzionalità supportate in questa release sono elencate nelle [note sulla release 17.7.1](#). Per tutte le funzionalità e i componenti hardware supportati a partire dalla versione 17.7.1, si consiglia di utilizzare 17.9.4 + SMU_CSCwh87343 + APSP (se necessario) O 17.9.4a + APSP (se necessario)

 Attenzione: la versione 17.7.1 è influenzata da [CSCwb13784](#) che impedisce l'unione degli access point wave 2 e 11ax se l'MTU del percorso scende al di sotto dei 1000 byte

Bengaluru 17.6

Cisco IOS XE 17.6.x è un treno con più MR, che ha una vita lunga. **C'è solo un altro MR previsto per il treno 17.6 solo per le correzioni di sicurezza.** Fare riferimento al [bollettino di fine del ciclo di vita della versione 17.6](#). Cisco consiglia di migrare alla versione 17.9.5 per tutte le distribuzioni.

17.6.7

Cisco IOS XE 17.6.7 è una versione solo per la correzione di bug. Questa è la release consigliata se si deve attenersi alla formazione software 17.6.

17.6.6 bis

Cisco IOS XE 17.6.6a corregge [CSCwh87343](#): vulnerabilità dell'escalation dei privilegi dell'interfaccia utente Web del software Cisco IOS XE. sostituisce 17.6.6.

17.6.6

Cisco IOS XE 17.6.6 è una versione solo per la correzione di bug.

17.6.5

Cisco IOS XE 17.6.5 è una versione solo per la correzione di bug e aggiunge la configurazione, in Policy Profile, per disabilitare l'accounting provvisorio. 17.6.5

17.6.4

Cisco IOS XE 17.6.4 è una versione solo per la correzione di bug e aggiunge la configurazione, in AP Join Profile, per abilitare la console seriale AP. Diverse correzioni di bug critici e il supporto per le versioni più recenti di alcuni punti di accesso Catalyst WiFi6 (fare riferimento alla [notifica sul campo 72424](#)) sono disponibili nella versione 17.6.4. Cisco consiglia di eseguire la migrazione a 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O 17.9.4a + APSP (in base alle esigenze)

17.6.4 PSP1

17.6.4 L'APSP fornisce una correzione per [CSCwd80290](#) che consente agli IW3700 AP di collegarsi al WLC anche dopo il 4 dicembre 2022. Per ulteriori informazioni, consultare il sito <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> e la notifica sul campo FN72524.

17.6.3

Cisco IOS XE 17.6.3 è una release che contiene esclusivamente correzioni di bug. Include tutte le correzioni della versione 17.3.5a + la correzione per [CSCwb13784](#).

Per i clienti che utilizzano la posizione con CMX o DNA Spaces, tenere presente [CSCwb65054](#). SMU (hot patch) pubblicato su cisco.com.

Molte correzioni di bug vengono fornite tramite patch SMU nella versione 17.6.3 e il supporto per le versioni più recenti di alcuni punti di accesso Catalyst WiFi6 (fare riferimento alla [notifica sul campo 72424](#)) è disponibile nella versione 17.6.4. Cisco consiglia di migrare alla versione 17.9.4 + SMU_CSCwh87343 + APSP (a seconda delle esigenze) O alla versione 17.9.4a + APSP (a

seconda delle esigenze)

17.6.2

Cisco IOS XE 17.6.2 aggiunge il supporto per alcune funzionalità.

- Supporto di 802.11 con autenticazione Web su errore autenticazione MAC
- Supporto Mesh e Mesh + Flex sui punti di accesso esterni C9124AXI/E/D
- Limitazione della velocità bidirezionale per client sui punti di accesso 802.11ac wave 2 e 11ax Catalyst

Molti bug critici della versione 17.6.2, ad esempio [CSCwb13784](#) che impedisce l'unione degli access point wave 2 e 11ax se la MTU del percorso scende al di sotto dei 1000 byte, vengono risolti nella versione 17.6.4. Cisco consiglia di eseguire la migrazione a 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O 17.9.4a + APSP (in base alle esigenze)

17.6.1

Le nuove funzionalità supportate in questa release sono documentate nelle [note sulla release 17.6](#). 17.6.1 è vulnerabile a diversi difetti critici e deve essere evitato.

Bengaluru 17.5.1

Cisco IOS XE 17.5.1 è una release di breve durata senza release di manutenzione pianificate. Vedere [17.5 End of Life Bulletin](#) L'elenco delle funzionalità supportate in questa release è riportato nelle [note sulla release 17.5](#). Per tutti i nuovi componenti hardware e le funzionalità supportate a partire dalla versione 17.5, Cisco consiglia di eseguire la migrazione alla versione 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O alla versione 17.9.4a + APSP (in base alle esigenze)

Bengaluru 17.4.1

Cisco IOS XE 17.4.1 è una release di breve durata senza release di manutenzione pianificate. Consultare l'[Avviso di fine vita della release 17.4](#). L'elenco delle funzionalità supportate in 17.4 sono elencate nelle [Note sulla versione 17.4](#). Per tutti i nuovi componenti hardware e le funzionalità supportate a partire dalla versione 17.4, Cisco consiglia di migrare alla versione 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O alla versione 17.9.4a + APSP (in base alle esigenze)

Amsterdam 17.3

Cisco IOS XE 17.3.x è un treno longevo con diverse versioni di manutenzione (MR). La versione 17.3 ha raggiunto la fine della manutenzione del software, come documentato nel [bollettino di fine ciclo di vita della versione 17.3](#). L'ultimo MR per 17.3 è una versione solo psirt prevista per settembre 2023. [Cisco consiglia di migrare alla versione 17.9.5 per tutte le distribuzioni se si utilizza una versione precedente.](#)

17.3.7

Cisco IOS XE 17.3.7 è l'ultimo bug-fix MR nella release train della versione 17.3. Per i clienti che desiderano rimanere sul treno della versione 17.3, Cisco consiglia la versione 17.3.7.

17.3.6

Cisco IOS XE 17.3.6 è principalmente una versione per la risoluzione dei bug. Aggiunge il supporto per

- Mesh e funzione mesh+flex per access point 9124 AXI/E/D
- Versioni più recenti (VID) di alcuni punti di accesso Catalyst WiFi6 (fare riferimento alla [Notifica 72424](#)).

17.3.6 PSP7

APSP7 fornisce le correzioni IOS in APSP5 e le correzioni AP COS in APSP6 come patch unificata.

17.3.6 APSP6 tramite [CSCwd89180](#)

17.3.6 APSP6 sostituisce 17.3.6 APSP2 e corregge più punti di accesso COS (11ac wave2 e Catalyst 11ax) difetti:

[CSCvx32806](#) COS-AP bloccati in bootloop a causa di un errore di verifica checksum immagine
[CSCwc32182](#) AP 1852 Radio Firmware Crash (SF 06029787/06121536/06208256)

[CSCwc89719](#) AP1832 arrestato in modo anomalo a causa di un errore radio (ripristino radio non riuscito) (SF#06180501)

[CSCvz9036](#) Access Point Cisco - Bypass VLAN da VLAN nativa

[CSCwd37092](#): download TCP lenti, autenticazione TLS non riuscita nella serie 8.10.181.0/17.3.6 - 2800/3800/4800

[CSCwc78435](#) 9130 invio di un elenco di canali non corretto in un evento DFS fuori banda che causa problemi di connettività client

[CSCwc88148](#) Miglioramenti aggiuntivi per il problema di sospensione mac ([CSCwc72194](#)) sul lato driver.

17.3.6 APSP5 tramite [CSCwd83653](#)

17.3.6 APSP5 fornisce la correzione per l'ID bug Cisco [CSCwd80290](#) che consente agli access point Cisco IOS di collegarsi al WLC anche dopo il 4 dicembre 2022. Per ulteriori informazioni, consultare il sito <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> e la notifica sul campo FN72524.

17.3.6 APSP2 tramite [CSCwd40096](#)

17.3.6 APSP2 fornisce la correzione per l'ID bug Cisco [CSCwd37092](#)

Sintomo: download lenti e errori di autenticazione EAP-TLS per access point serie 2800/3800/4800/1560/6300. Per confermare il bug, eseguire il comando `#show controllers nss status` sull'access point e verificare se il contatore `INNER_CAPWAP_RES_FAILED` è in aumento

Soluzione. Nessuna. Si è verificato un problema di download TCP solo su C9800 quando `tcp-adjust-mss 1250` è stato esplicitamente disabilitato in AP Join Profile. L'abilitazione di questa impostazione impedisce download TCP lenti, ma la lentezza di download UDP e gli errori EAP-TLS persistono.

Include anche la correzione per l'ID bug Cisco [CSCvz9036](#) e l'ID bug Cisco [CSCwc78435](#).

17.3.5 ter

Cisco IOS XE 17.3.5b è un'iterazione aggiornata della versione 17.3.5a che include le correzioni dei bug fornite tramite patch SMU e l'immagine di escalation della versione 17.3.5a. Per l'elenco completo, fare riferimento [a Difetti risolti nella versione 17.3.5b](#).

17.3.5 bis

Cisco IOS XE 17.3.5a: alcune importanti correzioni, tra cui

- Correzioni per trigger noti di CPU elevata in WNCd (tra cui sonde, tempesta ARP)
- Assegnazione di priorità CAPWAP keepalive per evitare che gli access point scendano quando si verificano picchi di utilizzo della CPU WNCd.
- Syslog per diagnosticare quando SSID interrompe la trasmissione e il meccanismo di ripristino della CLI. Vedere [CSCwb01162](#).

 **Attenzione:** l'immagine 17.3.5a CCO è influenzata dal [CSCwb13784](#) che impedisce l'unione dei punti di accesso wave 2 e 11ax se la MTU del percorso è inferiore a 1000 byte e impedisce l'unione dei punti di accesso Cisco IOS (1700/2700/3700) se la MTU del percorso è inferiore a 1500 byte.
Correzione: SMU (hot patch) pubblicato su [cisco.com](#) fornisce la correzione per il problema ed è obbligatorio da applicare.

17.3.4c

Cisco IOS XE 17.3.4c risolve diversi bug critici e di ampia portata della versione 17.3.4.

17.3.4

Cisco IOS XE 17.3.4 è una release che contiene esclusivamente correzioni di bug.

 **Nota:** se si utilizza la versione 17.3.3, le distribuzioni con C9130 e C9124s devono essere aggiornate alla versione 17.3.4c prima di essere aggiornate alla versione 17.8.1 e 17.9.1.

17.3.3

Cisco IOS XE 17.3.3 è una release che contiene esclusivamente correzioni di bug.

 **Attenzione:** 17.3.3 è vulnerabile a [CSCvy11981](#)

Sintomo: arresto anomalo WNCD

Trigger: se il nome di un punto di accesso è composto da 32 o più caratteri, la memoria potrebbe essere danneggiata e questo può causare il blocco

Soluzione. Assicurarsi che il numero di caratteri del nome dell'access point sia minore o uguale a 31.

17.3.2a

Cisco IOS XE 17.3.2a, sebbene sia una release di manutenzione, introduce alcune funzionalità oltre a correggere i bug, tra cui:

- Smart Licensing using Policy [configurazione GUI disponibile solo in 17.4.1]
- OEAP Personal SSID
- AP Authorization using Serial Number [estesa a tutti gli access point oltre a quelli presenti nel certificato wlancc+FIPS +LSC]
- Assurance and IoT Services Coexistence Without iCAP
- TLS tunnel to DNA-C on Cloud

17.3.1

Cisco IOS XE 17.3.1 ha introdotto il supporto per questi hardware e soluzioni

- Access point 9105I e 9105W
- Modello con velocità di trasmissione superiore su 9800CL
- Embedded Wireless sugli switch Catalyst 9k (non SDA)
- User Defined Network (UDN) e UDN Mobile Application
- Gestione BLE sul controller
- Gestione dei moduli IOT

Per l'elenco completo, fare riferimento alle [Note sulla versione 17.3.](#)

Amsterdam 17.2.1

Cisco IOS XE 17.2.1 è una serie di release di breve durata senza release di manutenzione pianificate. Vedere l' [Avviso di fine vita della release 17.2.](#) Per tutte le release 17.2.x per C9800, si rimanda all'[Avviso tecnico FN70577](#) e a [CSCvu24770](#) . Cisco consiglia di eseguire la migrazione a 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O 17.9.4a + APSP (in base alle esigenze) per tutte le implementazioni.

Amsterdam 17.1.1

Cisco IOS XE 17.1.1 è una release di breve durata senza release di manutenzione pianificate. Vedere l'[Avviso di fine vita della release 17.1](#). Per tutte le release 17.2.x per C9800, si rimanda all'[Avviso tecnico FN70577](#) e a [CSCvu24770](#). Cisco consiglia di eseguire la migrazione a 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O 17.9.4a + APSP (in base alle esigenze) per tutte le implementazioni.

Gibraltar 16.12

Cisco IOS XE 16.12 è la prima release train di lunga durata per 9800. La versione 16.12.1 ha introdotto il supporto per questi hardware e soluzioni.

- 9800-L
- 9800-CL su Google Cloud
- 9120AXE, 9130AXI
- Embedded Wireless Controller trasformati in access point Catalyst (EWC-AP)

16.12.8

Tutte le versioni 16.12.x dalla 16.12.2 alla 16.12.7 sono versioni per la sola correzione di bug. 16.12.8 è l'ultimo MR pianificato in questo treno. Consultare l'Avviso di fine vita della release 16.12. [Cisco consiglia di migrare alla versione 17.9.5 per tutte le implementazioni.](#)

 **Nota:** tutte le versioni 16.12.x precedenti alla 16.12.4a (16.12.1, 16.12.1s, 16.12.1t, 16.12.2s, 16.12.2t, 16.12.3, 16.12.3s) vengono rinviate all'indirizzo [CSCvu24770](#).

Gibraltar 16.11.1

Cisco IOS XE 16.11.1 è una release di breve durata senza release di manutenzione pianificate. Fare riferimento al [Bollettino di fine ciclo di vita](#). Per tutte le funzionalità della versione 16.x, Cisco consiglia di migrare alla versione 17.9.4 + SMU_CSCwh87343 + APSP (in base alle esigenze) O alla versione 17.9.4a + APSP (in base alle esigenze) per tutte le implementazioni

Gibraltar 16.10.1

Cisco IOS XE 16.10.1 è la prima versione del software Cisco IOS XE che supporta ufficialmente gli SKU Catalyst 9800 (appliance: 9800-40, 9800-80; 9800 su cloud privato/pubblico; 9800-CL, nonché software 9800 sugli switch Catalyst 9300). Cisco IOS XE 16.10.1e è la prima release a supportare l'integrazione di Cisco DNA Center con Catalyst 9800. Si tratta di una release di breve durata senza release di manutenzione pianificate. Fare riferimento al [Bollettino di fine ciclo di vita](#). Per tutte le funzionalità della versione 16.x, Cisco consiglia di migrare alla versione 17.9.4 + SMU_CSCwh87343 + APSP (a seconda delle esigenze) O 17.9.4a + APSP (a seconda delle esigenze) per tutte le implementazioni.

Firmware programmabile sul campo (FPGA) sui WLC 9800

Sui WLC Catalyst 9800 fisici (9800L, 9800-40, 9800-80), oltre a IOS-XE, esistono altre due parti di

software che possono essere aggiornate.

- ROM Monitor (ROMMON): è il programma bootstrap che inizializza il dispositivo e avvia il software IOS-XE sull'appliance C9800. La versione ROMMON in esecuzione sull'appliance può essere controllata con questo comando.

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

- PHY: si riferisce al livello fisico, in particolare al modulo Shared Port Adapter (SPA) che supporta la distribuzione front-end e le porte di uplink sulle appliance C9800. È possibile visualizzare la versione PHY in esecuzione sul dispositivo con questo comando.

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

Il nuovo firmware viene in genere rilasciato per proteggere lo stato del sistema (sensori di temperatura, ventola, alimentatore e così via) e per risolvere i problemi di inoltro dei dati in entrata e in uscita dalle porte fisiche. [Cisco consiglia di aggiornare il firmware FPGA alla versione più recente disponibile](#). Procedura di aggiornamento insieme ai difetti specifici per i quali è stato rilasciato il nuovo firmware, se documentato in occasione dell'[aggiornamento C9800 FPGA](#). La tabella 1 elenca le versioni per ciascuna piattaforma.

	ROMMON	Ethernet PHY	Fiber PHY
9800-L-F	16.12(3r)	N/D	17.11.1
9800-L-C	16.12(3r)	17.11.1	N/D
9800-40	17.7(3r)	N/D	16.0.0
9800-80	17.3(3r)	N/D	16.0.0

Manutenzione del software High Availability sui WLC 9800

C9800 offre diverse funzionalità che garantiscono la disponibilità durante la fase di manutenzione del software per tutta la durata dell'implementazione. Queste funzionalità includono In-Service Software Upgrade (ISSU), aggiornamenti di access point in sequenza, hot patch e cold patch per risolvere i difetti WLC o gli avvisi PSIRT (Product Security Incident Response Team), patch per risolvere problemi specifici degli access point e per supportare i nuovi modelli di access point sul software del controller esistente.

ISSU

Il supporto ISSU è stato introdotto nella release 17.3.1 ed è limitato alle release di lunga durata

(17.3.x, 17.6.x e 17.9.x). ISSU quindi funziona:

1. Nelle principali release di lunga durata, ad esempio dalla 17.3.x alla 17.3.y, dalla 17.6.x alla 17.6.y e dalla 17.9.x alla 17.9.y.
2. Tra le principali release di lunga durata, ad esempio dalla 17.3.x alla 17.6.x, dalla 17.3.x alla 17.9.x.

Nota: questo numero è limitato a due versioni di lunga durata dopo la versione di lunga durata attualmente supportata.

ISSU NON è supportato:

1. Nelle release secondarie della serie di release di breve durata, ad esempio dalla 17.4.x alla 17.4.y o dalla 17.5.x alla 17.5.y.
2. Tra le release principali e secondarie della serie di release di breve durata, ad esempio dalla 17.4.x alla 17.5.x.
3. Tra le release di lunga e breve durata, dalla 17.3.x alla 17.4.x o dalla 17.5.x alla 17.6.x.

Patch SMU (Software Maintenance Upgrade)

C9800 supporta l'applicazione di cold patch e hot patch che prevedono l'uso di file SMU (Software Maintenance Upgrade) contenenti le correzioni dei bug.

- Hot patch: non è necessario ricaricare il sistema, il WLC e gli access point continuano a funzionare. In caso di coppia di controller 9800 con SSO (Stateful Switchover), il processo di installazione SMU applica la patch a entrambi i dispositivi.
- Cold patch: è necessario ricaricare il sistema. In caso di una coppia di controller 9800 SSO, è possibile applicare la cold patch senza interrompere l'operatività.

Service Pack per access point

Le correzioni dei difetti software sugli access point (AP) possono essere fornite tramite appositi pacchetti di servizi, o APSP (Access Point Service Pack). I Service Pack richiedono il ricaricamento degli access point, ma non del WLC 9800.

Device Pack per access point

I Device Pack per access point, o APDP (Access Point Device Pack) permettono di supportare i nuovi modelli di access point sul software del controller WLC esistente senza doverlo aggiornare. Questo access point supporta solo le funzionalità disponibili nel codice WLC esistente.

Linee guida e requisiti

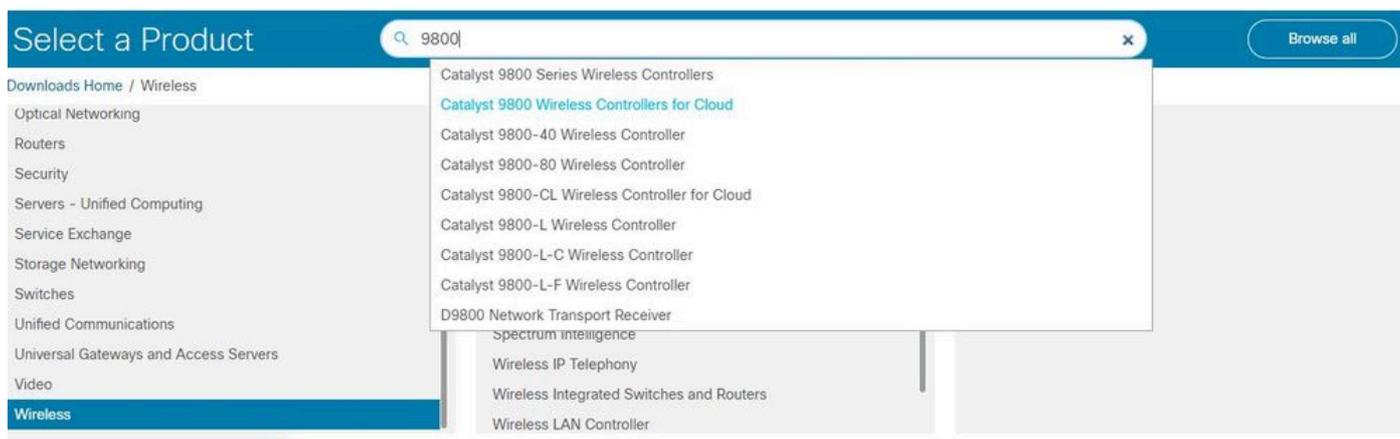
1. Le patch SMU vengono generate solo per le versioni a lunga durata come 16.12, 17.3, 17.6, 17.9 e così via dopo la release MD.
2. Gli aggiornamenti SMU possono essere applicati solo sui WLC 9800 con almeno una licenza Network Advantage. Fare riferimento alla [Matrice delle funzionalità wireless per le diverse licenze.](#)

3. Gli aggiornamenti SMU applicabili alla maggior parte delle implementazioni sono pubblicati sul sito cisco.com e possono essere scaricati autonomamente dai clienti.
4. Non è possibile applicare un file SMU o una patch per correggere tutti i bug. L'applicabilità della patch è determinata in genere dalle modifiche al software provocate dalla correzione dei bug.
5. L'applicabilità dell'SMU è valutata per difetto. Se lo switch C9800 è idoneo per una patch SMU, in base alla licenza e se è necessaria una SMU per un difetto specifico, rivolgersi al Technical Assistance Center (TAC) di Cisco per ottenere una valutazione del bug.

Per ulteriori dettagli su queste funzionalità, consultare la [Guida all'applicazione delle patch sui WLC C9800](#).

Ubicazione delle immagini SMU, APSP e APDP per i vari controller 9800 sul sito cisco.com

Passaggio 1. Accedere a [Download - Home](#), quindi cercare 9800 nella barra di ricerca per Selezionare un prodotto, quindi scegliere il fattore di forma 9800 applicabile.



Passaggio 2. Dal menu Tipo di software, selezionare SMU o APSP o APDP in base alle esigenze.

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](#)

Nota per Software Defined Access (SDA)

Fare riferimento sempre alla [Matrice di compatibilità SDA per la combinazione di codice consigliata per ottimizzare il funzionamento dell'SDA](#). Nella matrice di compatibilità sono elencate le combinazioni di codice specifiche di Cisco DNA Center, Identity Service Engine (ISE), switch, router e Wireless LAN Controller che sono state testate dal team SDA Solution Test di Cisco.

Inter Release Controller Mobility (IRCM)

- IRCM non è supportato sui controller 2504/7510/vWLC e solo sulle piattaforme 5508/8510/5520/8540/3504.
- Per la compatibilità IRCM (Inter-Release Controller Mobility) con WLC AireOS,
 - TAC consiglia AireOS 8.10.190.0 per tutte le implementazioni.
 - Per le distribuzioni con WLC o Access Point precedenti nel proprio ambiente, che non possono essere aggiornate oltre AireOS 8.5, TAC consiglia il codice IRCM [8.5.182.108 \(post nascosto\)](#).

Nota: non tutte le versioni con codice 8.5 supportano IRCM. Le versioni 8.5 IRCM disponibili sul sito cisco.com includono 8.5.164.0, 8.5.164.216, 8.5.176.0, 8.5.176.1, 8.5.176.2, 8.5.182.104.

Per il software AireOS consigliato, fare riferimento a:

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

[recommended-aires.html](#)

Funzionalità supportate sui Catalyst serie 9800 Wireless LAN Controller

[Note sulla release](#)

[Elenco delle funzionalità di Cisco IOS XE Wireless per release](#)

[Matrice per il confronto tra funzionalità da AireOS a Cisco IOS XE](#)

[Matrice delle funzionalità Flexconnect per gli access point wave2 e 11ax](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).