Catalyst 9800コントローラのアップグレードとダウングレード：ヒント

内容

はじめに

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(WLC)をアップグレードまたはダウングレードする際に注意する点について説明します。

続行する前に

このドキュメントは、アップグレード時に常に使用する必要があるリリースノートの置き換えを目的とするものではありません。このドキュメントの目的は、複数のリリース間で最も影響の大きい変更点を強調することにより、複数のリリースを通じてアップグレードを促進することです。

このドキュメントは、ターゲットソフトウェアリリースのリリースノートを読む方法を置き換えるものではありません。アップグレードを進める前に、設定をバックアップし、必要なすべての予防措置を講じてください。

デフォルトでは、9800のHTTPサーバは特定の証明書/トラストポイントに静的にマッピングされないため、アップグレード後に変更が発生する可能性があります。 アップグレードする前に、設定でHTTPサーバを静的トラストポイント（目的で発行した証明書、またはその他のMIC証明書が望ましい）に設定します。

エンジニアリング特別バージョンの特別なケース

エンジニアリングスペシャルビルドは、これらのビルドからのISSUアップグレードをサポートしません。このドキュメントでは、Cisco.comに公開されたパブリックリリースのみを取り上げています。そのため、エンジニアリングスペシャルビルドをご利用の場合は、リリースノートを参照して、アップグレードに関する疑問をすべて解決してください。

アップグレード

目的の宛先ソフトウェアバージョンの下の注を直接読むことができます。いくつかのリリースで適用可能なヒントは、利便性のために毎回繰り返されます。一度に3つ以上のリリースをアップグレードしないでください。たとえば、16.12.1から17.3.2へのアップグレードについては、このドキュメントで説明していますが、16.12から17.4へのアップグレードについては説明していません。このようなシナリオでは、17.3に移動して17.3セクションの下の注を確認し、アップグレードを実行してから、17.4セクションを確認して2回目のアップグレードを準備します。最後に、このドキュメントでは、中間のメジャーリリースに進むことを前提としているため、3つのメジャーリリースがリリースされた後は、有効な場合でも、ここで説明するヒントは繰り返されません。

ジブラルタル

16.12.2

- Cisco IOS® XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピングの変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。

- AP名には31文字を超える文字は使用しないでください。AP名が32文字以上の場合、コントローラがクラッシュする可能性があります。

- OVAファイルをVMware ESXi 6.5に直接導入しないでください。OVAファイルを導入するには、OVFツールを使用することを推奨します。

16.12.3

- 16.12.3は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。 アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピングの変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。

- AP名には31文字を超える文字は使用しないでください。AP名が32文字以上の場合、コントローラがクラッシュする可能性があります。

- OVAファイルをVMware ESXi 6.5に直接導入しないでください。OVAファイルを導入するには、OVFツールを使用することをお勧めします。

16.12.4

- 16.12.3および17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード

（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピングの変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。

- AP名には31文字を超える文字は使用しないでください。AP名が32文字以上の場合、コントローラがクラッシュする可能性があります。

- OVAファイルをVMware ESXi 6.5に直接導入しないでください。OVAファイルを導入するには、OVFツールを使用することをお勧めします。

16.12.5、16.12.6a、および16.12.7

16.12.4リリースと同じです。

アムステルダム

17.1.1

- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。
- このリリースから、新しいゲートウェイ到達可能性チェックが導入されました。APは接続を確認するために、定期的にICMP工コー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。

17.2.1

- 16.12.3および17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされている

SFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンする可能性があります。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。
- 17.1以降では、新しいゲートウェイ到達可能性チェックが導入されています。APは接続を確認するために、定期的にICMPエコー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。

17.3.1

- 16.12.3と17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。
- 17.1以降では、新しいゲートウェイ到達可能性チェックが導入されました。APは接続を確認するために、定期的にICMPエコー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。
- FIPSモードを設定している場合は、Cisco IOS XE Amsterdam 17.3.xを以前のバージョンからアップグレードする前に`security wpa wpa1 cipher tkip`、すべてのWLANから設定を削除してください。この操作を行わないと、WLANセキュリティがTKIPに設定されますが、これはFIPSモードではサポートされていません。アップグレード後に、AESを使用してWLANを再設定する必要があります。
- Cisco IOS XE Amsterdam 17.3.1以降のCisco Catalyst 9800-CLワイヤレスコントローラでは

、新規導入に16 GBのディスク領域が必要です。17.3イメージを再インストールしてディスク領域サイズを増やすことができるだけです。
- Cisco IOS XE Amsterdam 17.3.1以降では、AP名は32文字までしか使用できません。
- （クライアントまたはAPの）ローカルMACアドレス認証では、17.3.1の時点で形式aaaabbbbcccc（セパレータなし）のみがサポートされています。これは、Web UIまたはCLIで区切り文字を使用してMACアドレスを追加すると、認証が失敗することを意味します。
- このリリース以降、APがWLCに加入できず、ゲートウェイにpingできず、ゲートウェイにARPを実行できない場合、APは4時間後にリロードされます（APをリブートするには、3つすべてのAPに障害が発生する必要があります）。これは、以前のリリースからの以前のICMPのみのゲートウェイ検証に対する機能拡張(Cisco Bug ID CSCvt89970)です。
- 17.3.1以降では、アクセスポイントの国コードを設定する新しい方法として、異なる国コードで何度も繰り返すことができるコマンドがWireless country <1 country code>あります。これにより、国コードの最大量を20よりも増やすことができます。これらのコマンドは引き続き存在しap country、引き続き機能しますが、将来のバージョンではWireless countryコマンドが廃止されるためap country、コマンドをコマンドに変更することを検討してください。

17.3.2

- 16.12.3および17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。
- 17.1以降では、新しいゲートウェイ到達可能性チェックが導入されました。APは接続を確認するために、定期的にICMPエコー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。
- FIPSモードを設定している場合は、Cisco IOS XE Amsterdam 17.3.xを以前のバージョンからアップグレードする前にsecurity wpa wpa1 cipher tkip、すべてのWLANから設定を削除してください。この操作を行わないと、WLANセキュリティがTKIPに設定されますが、これはFIPSモードではサポートされていません。アップグレード後に、AESを使用してWLANを再設定する必要があります。
- Cisco IOS XE Amsterdam 17.3.1以降のCisco Catalyst 9800-CLワイヤレスコントローラでは、新規導入に16 GBのディスク領域が必要です。17.3イメージを再インストールしてディスク領域サイズを増やすことができるだけです。

- Cisco IOS XE Amsterdam 17.3.1以降では、AP名は最大32文字までしか使用できません。
- （クライアントまたはAPの）ローカルMACアドレス認証では、17.3.1の時点で形式aaaabbbbcccc（セパレータなし）のみがサポートされています。これは、Web UIまたはCLIで区切り文字を使用してMACアドレスを追加すると、認証が失敗することを意味します。
- 17.3.1以降では、APがWLCに加入できず、ゲートウェイにpingできず、ゲートウェイにARPを実行できない場合、4時間後にAPがリロードされます（APをリブートするには、3つすべてのAPに障害が発生する必要があります）。これは、以前のリリースからの以前のICMP専用ゲートウェイ検証に対する機能拡張(Cisco Bug ID CSCvt89970)です。
- 17.3.1以降では、アクセスポイントの国コードを設定する新しい方法として、異なる国コードで何度も繰り返すことができるコマンドがWireless country <1 country code>あります。これにより、国コードの最大量を20より多く増やすことができます。これらのコマンドは引き続き存在しap country、実行されていますが、将来のバージョンではWireless countryコマンドが廃止されるためap country、コマンドをコマンドに変更することを検討してください。

17.3.3

- 16.12.3および17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。
- 17.1以降では、新しいゲートウェイ到達可能性チェックが導入されています。APは接続を確認するために、定期的にICMPエコー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。
- FIPSモードを設定している場合は、Cisco IOS XE Amsterdam 17.3.xを以前のバージョンからアップグレードする前にsecurity wpa wpa1 cipher tkip、すべてのWLANから設定を削除してください。この操作を行わないと、WLANセキュリティがTKIPに設定されますが、これはFIPSモードではサポートされていません。アップグレード後に、AESを使用してWLANを再設定する必要があります。
- Cisco IOS XE Amsterdam 17.3.1以降のCisco Catalyst 9800-CLワイヤレスコントローラでは、新規導入に16 GBのディスク領域が必要です。17.3イメージを再インストールしてディスク領域サイズを増やすことができるだけです。
- Cisco IOS XE Amsterdam 17.3.1以降では、AP名は32文字までしか使用できません。
- （クライアントまたはAPの）ローカルMACアドレス認証では、17.3.1の時点で形式

aaaabbbbcccc（セパレータなし）のみがサポートされています。これは、Web UIまたはCLIで区切り文字を使用してMACアドレスを追加すると、認証が失敗することを意味します。
- 17.3.1以降では、APがWLCに加入できず、ゲートウェイにpingできず、ゲートウェイにARPを実行できない場合、4時間後にAPがリロードされます（APをリブートするには、3つすべてのAPに障害が発生する必要があります）。これは、以前のリリースからの以前のICMP専用ゲートウェイ検証の機能拡張(Cisco Bug ID CSCvt89970)です。
- 17.3.1以降では、アクセスポイントの国コードを設定する新しい方法として、異なる国コードで何度も繰り返すことができるコマンドがWireless country <1 country code>あります。これにより、国コードの最大量を20よりも増やすことができます。これらのコマンドは現在も存在しap country、機能しますが、将来のバージョンでWireless countryは非推奨となるためap country、コマンドをコマンドに変更することを検討してください。
- APのホスト名が32文字を超えると、WLCがクラッシュする可能性があります(Cisco Bug ID CSCvy11981)。

17.3.4

- 16.12.3と17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。
- 17.1以降では、新しいゲートウェイ到達可能性チェックが導入されました。APは接続を確認するために、定期的にICMPエコー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。
- FIPSモードを設定している場合は、Cisco IOS XE Amsterdam 17.3.xを以前のバージョンからアップグレードする前にsecurity wpa wpa1 cipher tkip、すべてのWLANから設定を削除してください。この操作を行わないと、WLANセキュリティがTKIPに設定されますが、これはFIPSモードではサポートされていません。アップグレード後に、AESを使用してWLANを再設定する必要があります。
- Cisco IOS XE Amsterdam 17.3.1以降のCisco Catalyst 9800-CLワイヤレスコントローラでは、新規導入に16 GBのディスク領域が必要です。17.3イメージを再インストールしてディスク領域サイズを増やすことができるだけです。
- Cisco IOS XE Amsterdam 17.3.1以降では、AP名は最大32文字までしか使用できません。
- （クライアントまたはAPの）ローカルMACアドレス認証では、17.3.1の時点で形式

aaaabbbbcccc（セパレータなし）のみがサポートされています。これは、Web UIまたはCLIで区切り文字を使用してMACアドレスを追加すると、認証が失敗することを意味します。
- 17.3.1以降では、APsIはWLCに参加できず、ゲートウェイにpingできず、ゲートウェイにARPを実行できない場合、4時間後にリロードされます（APをリブートするには、3つすべてのAPが失敗する必要があります）。これは、以前のリリースからの以前のICMP専用ゲートウェイ検証に対する機能拡張(Cisco Bug ID CSCvt89970)です。
- 17.3.1以降、アクセスポイントの国コードを設定する新しい方法は、Wireless country <1 country code>国コードを変えて複数回繰り返すことができるコマンドです。これにより、国コードの最大量を20よりも増やすことができます。これらのコマンドは現在も存在しap country、機能しますが、将来のバージョンで廃止されるWireless countryと考えられるためap country、コマンドに変更することを検討してください。
- 17.3.4以降にアップグレードする場合は、16.12.5rブートローダ/rommonを適用可能なコントローラ(9800-80)にインストールすることをお勧めします。（9800-40には現時点でROMMON 16.12.5rがないため、ROMMONのアップグレードは必要ありません）。
- Cisco IOS XE Bengaluru 17.3.xからISSUを使用する任意のリリースへのコントローラのアップグレードは、 snmp-server enable traps hsrpコマンドが設定されます。ISSUアップグレードを開始する前にsnmp-server enable traps hsrp、必ず設定からコマンドを削除してください。これは、Cisco IOS XEベンガルール17.4.xからsnmp-server enable traps hsrp、このコマンドが削除されているためです。

- Cisco IOS XE 17.3.x以降のリリースにアップグレードする際に、コマンドが有効になっている場合ip http active-session-modules none、HTTPSを使用してコントローラのGUIにアクセスできません。HTTPSを使用してGUIにアクセスするには、次のコマンドを実行します。

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

17.3.5

- Cisco Bug ID CSCwb13784が原因で、パスMTUが1500バイトより小さい場合、APが加入できない可能性があります。この問題を修正するには、17.3.5用のSMUパッチをダウンロードします。
- 16.12.3と17.2.1は、ドキュメントにサポート対象として記載されているSFPのみのサポートを強制する最初のリリースです。リストされていないSFPが原因で、ポートがダウンします。アップグレード後にデータポートがダウンするのを防ぐため、サポートされているSFPのリストを確認し、SFPの互換性を確認します。
- 16.12.1リリースの場合、このリリースのアップグレードファイルはHTTPアップロード（Web UIのアップグレード時）には大きすぎる可能性があります。別の転送方法を使用するか、16.12.2に進みます。16.12.2では、Web UIを介してアップロードされる、より大きなファイルがサポートされています。
- Cisco IOS XE Gibraltar 16.12.2sからは、デフォルトポリシータグの下のデフォルトポリシープロファイルへの自動WLANマッピングが削除されています。Cisco IOS XE Gibraltar 16.12.2sよりも前のリリースからアップグレードする場合、ワイヤレスネットワークでデフォルトのポリシータグが使用されていると、デフォルトのマッピング変更によりポリシータグがダウンします。ネットワーク動作を復元するには、必要なWLANをデフォルトポリシータグの下のポリシーマッピングに追加します。

- 17.1以降では、新しいゲートウェイ到達可能性チェックが導入されています。APは接続を確認するために、定期的にICMPエコー要求(ping)をデフォルトゲートウェイに送信します。APとデフォルトゲートウェイの間でICMP pingを許可するには、APとデフォルトゲートウェイ（ACLなど）の間のトラフィックフィルタリングを確認する必要があります。これらのpingがブロックされると、コントローラとAP間の接続がアクティブであっても、APは4時間間隔でリロードします。
- FIPSモードを設定している場合は、Cisco IOS XE Amsterdam 17.3.xを以前のバージョンからアップグレードする前に`security wpa wpa1 cipher tkip`、すべてのWLANから設定を削除してください。この操作を行わないと、WLANセキュリティがTKIPに設定されますが、これはFIPSモードではサポートされていません。アップグレード後に、AESを使用してWLANを再設定する必要があります。
- Cisco IOS XE Amsterdam 17.3.1以降のCisco Catalyst 9800-CLワイヤレスコントローラでは、新規導入に16 GBのディスク領域が必要です。17.3イメージを再インストールしてディスク領域サイズを増やすことができるだけです。
- Cisco IOS XE Amsterdam 17.3.1以降では、AP名は32文字までしか使用できません。
- （クライアントまたはAPの）ローカルMACアドレス認証では、17.3.1の時点で形式`aaaabbbbcccc`（セパレータなし）のみがサポートされています。これは、Web UIまたはCLIで区切り文字を使用してMACアドレスを追加すると、認証が失敗することを意味します。
- 17.3.1以降では、APsIはWLCに参加できず、ゲートウェイにpingできず、ゲートウェイにARPを実行できない場合、4時間後にリロードされます（APのリブートには3つとも失敗する必要があります）。これは、以前のリリースからの以前のICMP専用ゲートウェイ検証に対する機能拡張(Cisco Bug ID CSCvt89970)です。
- 17.3.1以降、アクセスポイントの国コードを設定する新しい方法は、`Wireless country <1 country code>`国コードを変えて複数回繰り返すことができるコマンドです。これにより、国コードの最大量を20よりも増やすことができます。これらのコマンドは現在も存在し`ap country`、機能しますが、将来のバージョンで廃止される`Wireless country`と考えられるため`ap country`、コマンドに変更することを検討してください。
- 17.3.4以降にアップグレードする場合は、16.12.5rブートローダ/rommonを適用可能なコントローラ(9800-80)にインストールすることをお勧めします。（9800-40には現時点でROMMON 16.12.5rがないため、ROMMONのアップグレードは必要ありません）。
- Cisco IOS XE Bengaluru 17.3.xからISSUを使用する任意のリリースへのコントローラのアップグレードは、 `snmp-server enable traps hsrp`コマンドが設定されます。ISSUアップグレードを開始する前に`snmp-server enable traps hsrp`、必ず設定からコマンドを削除してください。これは、Cisco IOS XEベンガルール17.4.xから`snmp-server enable traps hsrp`、このコマンドが削除されているためです。

- Cisco IOS XE 17.3.x以降のリリースにアップグレードする際に、コマンドが有効になっている場合`ip http active-session-modules none`、HTTPSを使用してコントローラのGUIにアクセスできません。HTTPSを使用してGUIにアクセスするには、次のコマンドを実行します。
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist

ベンガルール

17.4.1

- 17.4.1以降では、Wave 1 Cisco IOSベースのAP(1700、2700、3700、1570)は、IW3700を除きサポートされません。
- 非WPA（ゲスト、オープン、またはCWA SSID）でAdaptive FTが設定されているWLANは、アップグレード後にシャットダウンできます。解決策は、アップグレードの前に適応型FT設定を削除することです(Cisco Bug ID CSCvx34349)。適応型FTの設定は非WPA SSIDでは意味がないため、削除しても何も失われません。
- APのホスト名が32文字を超えると、WLCがクラッシュする可能性があります(Cisco Bug ID CSCvy11981)。

17.5.1

- 17.4.1以降では、Wave 1 Cisco IOSベースのAP(1700、2700、3700、1570)は、IW3700を除きサポートされません。
- Cisco IOS XE Bengaluruリリース17.4.1以降では、テレメトリソリューションは、テレメトリデータのIPアドレスではなく、受信者アドレスの名前を提供します。これは追加オプションです。コントローラのダウングレードとそれに続くアップグレード中に、新しく名前を付けたレシーバを使用するアップグレードバージョンに問題がある可能性があり、これらがダウングレードで認識されません。新しい設定は拒否され、その後のアップグレードで失敗します。Cisco DNA Centerからアップグレードまたはダウングレードを実行すると、設定の消失を回避できます。
- 非WPA（ゲスト、オープン、またはCWA SSID）でAdaptive FTが設定されているWLANは、アップグレード後にシャットダウンできます。解決策は、アップグレードの前に適応型FT設定を削除することです(Cisco Bug ID CSCvx34349)。適応型FTの設定は非WPA SSIDでは意味がないため、削除しても何も失われません。
- APのホスト名が32文字を超えると、WLCがクラッシュする可能性があります(Cisco Bug ID CSCvy11981)。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。

- Cisco IOS XE 17.3.x以降のリリースにアップグレードする際に`ip http active-session-modules none`、コマンドが有効になっていると、HTTPSを使用してGUIにアクセスできません。HTTPSを使用してGUIにアクセスするには、次のコマンドを実行します。

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- リブートまたはシステムクラッシュの後にGUIから「ERR_SSL_VERSION_OR_CIPHER_MISMATCH」エラーが表示された場合は、トラストポイント証明書を再生成することをお勧めします。
- 新しい自己署名トラストポイントを生成する手順は、次のとおりです。

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

```
! use local or aaa as applicable.
```

17.6.1

- 17.4.1以降では、Wave 1 Cisco IOSベースのAP(1700、2700、3700、1570)は、IW3700を除きサポートされません。
- Cisco IOS XE Bengaluruリリース17.4.1以降では、テレメトリソリューションは、テレメトリデータのIPアドレスではなく、受信者アドレスの名前を提供します。これは追加オプションです。コントローラのダウングレードとそれに続くアップグレード中に、新しく名前を付けたレシーバを使用するアップグレードバージョンに問題がある可能性があり、これらがダウングレードで認識されません。新しい設定は拒否され、その後のアップグレードで失敗します。Cisco DNA Centerからアップグレードまたはダウングレードを実行すると、設定の消失を回避できます。
- 非WPA（ゲスト、オープン、またはCWA SSID）でAdaptive FTが設定されているWLANは、アップグレード後にシャットダウンできます。解決策は、アップグレードの前に適応型FT設定を削除することです(Cisco Bug ID CSCvx34349)。適応型FTの設定は非WPA SSIDでは意味がないため、削除しても何も失われません。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。
- 17.6.1以降のWLCに加入したAPは、8.10.162以降または8.5.176.2以降の8.5コードを実行しない限り、AireOS WLCに加入できません。
- 17.6.1以降にアップグレードする場合は、該当するコントローラ(9800-80)に16.12.5rブートローダ/rommonをインストールすることをお勧めします。（9800-40には現時点でROMMON 16.12.5rがないため、ROMMONのアップグレードは必要ありません）。
- Cisco IOS XE Bengaluru 17.3.xからISSUを使用する任意のリリースへのコントローラのアップグレードは、 snmp-server enable traps hsrpコマンドが設定されます。ISSUアップグレードを開始する前にsnmp-server enable traps hsrp、必ず設定からコマンドを削除してください。これは、Cisco IOS XEベンガルール17.4.xからsnmp-server enable traps hsrp、このコマンドが削除されているためです。

- Cisco IOS XE 17.3.x以降のリリースにアップグレードする際に、コマンドが有効になっている場合ip http active-session-modules none、コントローラのGUIへのHTTPSアクセスが機能しません

。HTTPSを使用してGUIにアクセスするには、次のコマンドを実行します。

- ip http session-module-list pkilist OPENRESTY_PKI
- ip http active-session-modules pkilist

- リブートまたはシステムクラッシュの後にGUIから「ERR_SSL_VERSION_OR_CIPHER_MISMATCH」エラーが表示された場合は、トラストポイント証明書を再生成することをお勧めします。
- 新しい自己署名トラストポイントを生成する手順は、次のとおりです。

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http securffwe-server ip http server ip http secure-server ip http authen
```

```
! use local or aaa as applicable.
```

17.6.2

- 17.4.1以降では、Wave 1 Cisco IOSベースのAP(1700、2700、3700、1570)は、IW3700を除きサポートされません。
- Cisco IOS XE Bengaluruリリース17.4.1以降では、テレメトリソリューションは、テレメトリデータのIPアドレスではなく、受信者アドレスの名前を提供します。これは追加オプションです。コントローラのダウングレードとそれに続くアップグレード中に、新しく名前を付けたレシーバを使用するアップグレードバージョンに問題がある可能性があり、これらがダウングレードで認識されません。新しい設定は拒否され、その後のアップグレードで失敗します。Cisco DNA Centerからアップグレードまたはダウングレードを実行すると、設定の消失を回避できます。
- 非WPA（ゲスト、オープン、またはCWA SSID）でAdaptive FTが設定されているWLANは、アップグレード後にシャットダウンできます。解決策は、アップグレードの前に適応型FT設定を削除することです(Cisco Bug ID CSCvx34349)。適応型FTの設定は非WPA SSIDでは意味がないため、削除しても何も失われません。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが

正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。

- 17.6.1以降のWLCに加入したAPは、8.10.162以降または8.5.176.2以降の8.5コードを実行しない限り、AireOS WLCに加入できません。
- 17.6.1以降にアップグレードする場合は、該当するコントローラ(9800-80)に16.12.5rブートローダ/rommonをインストールすることをお勧めします。（9800-40には現時点でrommon 16.12.5rがないため、rommonのアップグレードは必要ありません）。
- Cisco IOS XE Bengaluru 17.3.xからISSUを使用する任意のリリースへのコントローラのアップグレードは、 snmp-server enable traps hsrpコマンドが設定されます。ISSUアップグレードを開始する前にsnmp-server enable traps hsrp、必ず設定からコマンドを削除してください。これは、Cisco IOS XEベンガルール17.4.xからsnmp-server enable traps hsrp、このコマンドが削除されているためです。

- Cisco IOS XE 17.3.x以降のリリースにアップグレードする際に、コマンドが有効になっている場合ip http active-session-modules none、HTTPSコントローラのGUIアクセスが機能しません。HTTPSを使用してGUIにアクセスするには、次のコマンドを実行します。

    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist

- AP名には31文字を超える文字は使用しないでください。AP名が32文字以上の場合、コントローラがクラッシュする可能性があります。

- リブートまたはシステムクラッシュの後にGUIから「ERR_SSL_VERSION_OR_CIPHER_MISMATCH」エラーが表示された場合は、トラストポイント証明書を再生成することをお勧めします。

- 新しい自己署名トラストポイントを生成する手順は、次のとおりです。

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

```
! use local or aaa as applicable.
```

クパチーノ

このセクションでは、17.6.1以降からCupertinoリリースにアップグレードすることを前提としています。以前のリリースから直接アップグレードする場合は（サポートされている可能性があるため、リリースノートを確認してください）、17.3および17.6のセクションの警告をお読みください。

17.7.1

- AP名には31文字を超える文字は使用しないでください。AP名が32文字以上の場合、コントローラがクラッシュする可能性があります。
- 17.7.1 AP joinプロファイルでAP国コードを設定する必要がある
- Cisco Bug ID CSCvu22886により、9130または9124 APを使用している場合は、17.3.4よりも前のリリースから17.7.1以降にアップグレードするときは17.3.5aを通過する必要があります。
- Cisco IOS XE Cuppertino 17.7.1以降から、Cisco Catalyst 9800-CL Wireless Controllerに対して、Resource Utilization Measurement(RUM)レポートを完了し、製品インスタンスで少なくとも1回はACKが使用可能になっていることを確認します。これは、正しい最新の使用情報がCisco Smart Software Manager(CSSM)に反映されるようにするためです。これを行わないと、ライセンスレポートがACKされるまで、最大50台のAPが9800-CLに加入できます。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。

17.8.1

- AP名には31文字を超える文字は使用しないでください。AP名が32文字以上の場合、コントローラがクラッシュする可能性があります。
- 17.7.1 AP joinプロファイルでAP国コードを設定する必要がある
- Cisco Bug ID CSCvu22886により、9130または9124 APを使用している場合は、17.3.4よりも前のリリースから17.7.1以降にアップグレードする際に17.3.5aを通過する必要があります。
- Cisco Catalyst 9800-CLワイヤレスコントローラのCisco IOS XE Cuppertino 17.7.1以降では、RUMレポートを完了し、製品インスタンスで少なくとも1回はACKが使用可能であることを確認してください。これは、正しい最新の使用状況の情報がCSSMに反映されるようにするためです。これを行わないと、ライセンスレポートがACKされるまで、最大50台のAPが9800-CLに加入できます。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。

17.9.x

- Cisco IOS-XE 17.9.3を実行しているAPでは、ディレクトリに十分なスペースがないためにソフトウェアをアップグレードしようとすると、問題が発生する可能性があり/tmpます。APの領域がいっぱいになると/tmp、新しいAPイメージのダウンロードができなくなります。このような場合は、APをリブートすることを推奨します。

- WANリンク経由でソフトウェアをアップグレードすると、11AC Wave 2 APがブートループに陥る可能性があります。詳細については、https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.htmlを参照してください。

- 17.9.3以降のリリースでは、Cisco IOSベースのアクセスポイント（x700シリーズおよび1570）のサポートが復活しています。17.4と17.9.2の間ではサポートされていません。これらのAPのサポートは、通常の製品ライフサイクルサポートを超えるものではありません。Cisco.comの個々のサポート終了速報を参照してください。
- domainコマンドが設定されている場合、ISSUを使用したCisco IOS XE Bengaluru 17.3.xからCisco IOS XE Bengaluru 17.6.xまたはCisco IOS XE Cuppertino 17.9.x以降へのコントローラアップグレードが失敗する場合があります。domainコマンドはCisco IOS XEベンガルール17.6.xから削除されているため、ISSUのアップグレードを開始する前に必ずno domainコマンドを実行してください。
- Cisco Catalyst 9800-CLワイヤレスコントローラのCisco IOS XE Cuppertino 17.7.1以降では、RUMレポートを完了し、製品インスタンスで少なくとも1回はACKが使用可能であることを確認してください。これは、正しい最新の使用状況の情報がCSSMに反映されるようにするためです。これを行わないと、ライセンスレポートがACKされるまで、最大50台のAPが9800-CLに加入できます。
- 1500未満のフラグメンテーションは、Gi0(OOB)インターフェイスでワイヤレスクライアントによって生成されるRADIUSパケットではサポートされません。
- 17.3以降、9800-CLが正常に機能するには、16 GBのディスク領域が必要です。WLCインスタンスが8 GBのOVA（17.3より前）で開始された場合、サイズを動的に増加することはできません。唯一の方法は、17.3よりも後の日付のOVAから新しいWLCを作成することです。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。
- Cisco Catalyst 9800-Lワイヤレスコントローラは、ブート時にコンソールポートで受信したブレーク信号に応答できなくなり、ユーザがrommonにアクセスできなくなる場合があります。この問題は、2019年11月まで製造されたコントローラで、デフォルトのconfig-register設定が0x2102の場合に発生します。この問題は、config-registerを0x2002に設定すると回避できます。この問題は、Cisco Catalyst 9800-Lワイヤレスコントローラの ROMmon 16.12(3r)で修正されています。ROMMONをアップグレードする方法については、『Cisco Catalyst 9800シリーズワイヤレスコントローラ用のField Programmable Hardware Devices(FPD)のアップグレードUpgrading rommon for Cisco Catalyst 9800-L Wireless Controllers』のセクションを参照してください。

- リブートまたはシステムクラッシュの後にこのエラーメッセージが表示された場合は、トラストポイント証明書を再生成することをお勧めします。

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

新しい自己署名トラストポイント証明書を生成するには、次のコマンドを指定された順序で使用します。

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- コマンドを使用して、モビリティMACアドレスが設定されていることを確認しますwireless mobility mac-address。
- これらのプロトコルは、17.9のサービスポートでサポートされるようになりました。
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - コントローラGUI
  - DNS
  - ファイル転送
  - GNMI
  - HTTP
  - HTTPS
  - [LDAP]
  - CSSMと通信するためのSmart Licensing機能のライセンス
  - Netconf
  - NetFlow
  - NTP
  - RADIUS（CoAを含む）
  - Restconf

- SNMP
- SSH
- SYSLOG
- TACACS+

- 17.9用のAPイメージは、最初に許可されたAPフラッシュよりも大きいものです。17.9イメージのダウンロード時にAPに十分なスペースがないという苦情が出た場合は、リリースノートで説明されているように17.3.5経由のアップグレードパスを尊重しなかったか、APで古いAireOSイメージが稼働していることが原因である可能性があります。17.3.5以降のWLCを経由して移行するか、AireOSイメージを最新のものにアップグレードすると、APフラッシュのサイズが変更され、17.9イメージのダウンロードが可能になります。

ダブリン

17.10.1

- Cisco Centralized Key Management(CCKM)機能は、Cisco IOS XE Dublin 17.10.xでは廃止されています。
- Smart Call Homeは、ライセンスに関してSmart Transportを推奨しないため、廃止される予定です。

- Cisco IOS-XE 17.9.3以降を実行しているAPでは、ディレクトリに十分なスペースがないためにソフトウェアをアップグレードしようとすると問題が発生する可能性があり/tmpます。APの領域がいっぱいになると/tmp、新しいAPイメージのダウンロードができなくなります。このような場合は、APをリブートすることを推奨します。

  WANリンク経由でソフトウェアをアップグレードすると、Wave 2 APがブートループに陥る可能性があります。詳細については、https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.htmlを参照してください。

- Cisco IOS XE Cuppertino 17.7.1以降から、Cisco Catalyst 9800-CL Wireless Controllerに対して、RUMレポートを完了し、製品インスタンスで少なくとも1回はACKが使用可能になっていることを確認します。これは、正しい最新の使用状況の情報がCSSMに反映されるようにするためです。これを行わないと、ライセンスレポートがACKされるまで、最大50台のAPが9800-CLに加入できます。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。
- 1500未満のフラグメンテーションは、Gi0(OOB)インターフェイスでワイヤレスクライアントによって生成されるRADIUSパケットではサポートされません。
- 17.3以降、9800-CLが正常に機能するには、16 GBのディスク領域が必要です。WLCインスタンスが8 GBのOVA（17.3より前）で開始された場合、サイズを動的に増加することはできません。唯一の方法は、17.3よりも後の日付のOVAから新しいWLCを作成することです。
- Cisco Catalyst 9800-Lワイヤレスコントローラは、ブート時にコンソールポートで受信した

BREAK信号に応答できなくなり、ユーザがrommonにアクセスできなくなる場合があります。この問題は、2019年11月まで製造されたコントローラで、デフォルトのconfig-register設定が0x2102の場合に発生します。この問題は、config-registerを0x2002に設定すると回避できます。この問題は、Cisco Catalyst 9800-LワイヤレスコントローラのROMmon 16.12(3r)で修正されています。ROMMONをアップグレードする方法については、『Cisco Catalyst 9800シリーズワイヤレスコントローラのField Programmable Hardware Devicesのアップグレード』ドキュメントの「Cisco Catalyst 9800-Lワイヤレスコントローラの ROMMONのアップグレード」セクションを参照してください。

- リブートまたはシステムクラッシュの後にこのエラーメッセージが表示された場合は、トラストポイント証明書を再生成することをお勧めします。

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

新しい自己署名トラストポイント証明書を生成するには、次のコマンドを指定された順序で使用します。

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- コマンドを使用して、モビリティMACアドレスが設定されていることを確認しますwireless mobility mac-address。
- これらのプロトコルは、17.9のサービスポートでサポートされるようになりました。
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - コントローラGUI
  - DNS
  - ファイル転送

    - GNMI
    - HTTP
    - HTTPS
    - [LDAP]
    - CSSMと通信するためのSmart Licensing機能のライセンス
    - Netconf
    - NetFlow
    - NTP
    - RADIUS（CoAを含む）
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- 17.9用のAPイメージは、最初に許可されたAPフラッシュよりも大きいです。17.9イメージのダウンロード時にAPに十分なスペースがないという苦情が出た場合は、17.3.5までのアップグレードパスがリリースノートで説明されているとおりに守られていなかったか、APで古いAireOSイメージが稼働していることが原因と考えられます。17.3.5以降のWLCを通過するか、AireOSイメージを最新のものにアップグレードすると、APフラッシュのサイズが変更され、17.9イメージのダウンロードが可能になります。

17.11.1

- CCKM機能は、Cisco IOS XE Dublin 17.10.xでは廃止されています。
- Smart Call Homeは、ライセンスのSmart Transportのために廃止されつつあります
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。

- Cisco IOS-XE 17.9.3以降を実行しているAPでは、ディレクトリに十分なスペースがないためにソフトウェアをアップグレードしようとすると問題が発生する可能性があり/tmpます。APの領域がいっぱいになると/tmp、新しいAPイメージのダウンロードができなくなります。このような場合は、APをリブートすることを推奨します。

  WANリンク経由でソフトウェアをアップグレードすると、Wave 2 APがブートループに陥る可能性があります。詳細については、
  https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-

controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.htmlを参照してください。

- Cisco Catalyst 9800-CLワイヤレスコントローラのCisco IOS XE Cuppertino 17.7.1以降では、RUMレポートが完了し、製品インスタンスで少なくとも1回はACKが使用可能になっていることを確認してください。これは、正しい最新の使用状況の情報がCSSMに反映されるようにするためです。これを行わないと、ライセンスレポートがACKされるまで、最大50台のAPが9800-CLに加入できます。
- 1500未満のフラグメンテーションは、Gi0(OOB)インターフェイスでワイヤレスクライアントによって生成されるRADIUSパケットではサポートされません。
- 17.3以降、9800-CLが正常に機能するには、16 GBのディスク領域が必要です。WLCインスタンスが8 GBのOVA（17.3より前）で開始された場合、サイズを動的に増加することはできません。唯一の方法は、17.3よりも後の日付のOVAから新しいWLCを作成することです。
- Cisco Catalyst 9800-Lワイヤレスコントローラは、ブート時にコンソールポートで受信したブレーク信号に応答できなくなり、ユーザがrommonにアクセスできなくなる場合があります。この問題は、2019年11月まで製造されたコントローラで、デフォルトのconfig-register設定が0x2102の場合に発生します。config-registerを0x2002に設定すると回避できます。この問題は、Cisco Catalyst 9800-LワイヤレスコントローラのROMmon 16.12(3r)で修正されています。ROMMONをアップグレードする方法については、『Cisco Catalyst 9800シリーズワイヤレスコントローラのField Programmable Hardware Devicesのアップグレード』ドキュメントの「Cisco Catalyst 9800-LワイヤレスコントローラのROMMONのアップグレード」セクションを参照してください。

- リブートまたはシステムクラッシュの後にこのエラーメッセージが表示された場合は、トラストポイント証明書を再生成することをお勧めします。

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

新しい自己署名トラストポイント証明書を生成するには、次のコマンドを指定された順序で使用します。

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- コマンドを使用して、モビリティMACアドレスが設定されていることを確認しますwireless mobility mac-address。
- これらのプロトコルは、17.9のサービスポートでサポートされるようになりました。
    - Cisco DNA Center
    - Cisco Smart Software Manager
    - Cisco Prime Infrastructure
    - Telnet
    - コントローラGUI
    - DNS
    - ファイル転送
    - GNMI
    - HTTP
    - HTTPS
    - [LDAP]
    - CSSMと通信するためのSmart Licensing機能のライセンス
    - Netconf
    - NetFlow
    - NTP
    - RADIUS（CoAを含む）
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- 17.9用のAPイメージは、最初に許可されたAPフラッシュよりも大きいです。17.9イメージのダウンロード時にAPに十分なスペースがないという苦情が出た場合は、17.3.5までのアップグレードパスがリリースノートで説明されているとおりに守られていなかったか、APで古いAireOSイメージが稼働していることが原因と考えられます。17.3.5以降のWLCを通過するか、AireOSイメージを最新のものにアップグレードすると、APフラッシュのサイ

ズが変更され、17.9イメージのダウンロードが可能になります。

17.12.1

- CCKM機能は、Cisco IOS XE Dublin 17.10.xでは廃止されています。
- Smart Call Homeは、ライセンスに関してSmart Transportを推奨しないため、廃止される予定です。
- GUIをあるリリースから別のリリースにアップグレードする場合は、すべてのGUIページが正しくリロードされるように、ブラウザのキャッシュをクリアすることをお勧めします。

- Cisco IOS-XE 17.9.3以降を実行しているAPでは、ディレクトリに十分なスペースがないためにソフトウェアをアップグレードしようとすると問題が発生する可能性があり/tmpます。APの領域がいっぱいになると/tmp、新しいAPイメージのダウンロードができなくなります。このような場合は、APをリブートすることを推奨します。

  WANリンク経由でソフトウェアをアップグレードすると、Wave 2 APがブートループに陥る可能性があります。詳細については、https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.htmlを参照してください。

- 17.12.1以降のリリースでは、Cisco IOSベースのアクセスポイント（x700シリーズおよび1570）のサポートが復活しています。17.4と17.9.2の間ではサポートされていません。これらのAPのサポートは、通常の製品ライフサイクルサポートを超えるものではありません。Cisco.comの個々のサポート終了速報を参照してください。
- Cisco Catalyst 9800-CLワイヤレスコントローラのCisco IOS XE Cuppertino 17.7.1以降では、RUMレポートを完了し、製品インスタンスで少なくとも1回はACKが使用可能であることを確認してください。これは、正しい最新の使用状況の情報がCSSMに反映されるようにするためです。これを行わないと、ライセンスレポートがACKされるまで、最大50台のAPが9800-CLに加入できます。
- 1500未満のフラグメンテーションは、Gi0(OOB)インターフェイスでワイヤレスクライアントによって生成されるRADIUSパケットではサポートされません。
- 17.3以降、9800-CLが正常に機能するには、16 GBのディスク領域が必要です。WLCインスタンスが8 GBのOVA（17.3より前）で開始された場合、サイズを動的に増加することはできません。唯一の方法は、17.3よりも後の日付のOVAから新しいWLCを作成することです。
- Cisco Catalyst 9800-Lワイヤレスコントローラは、ブート時にコンソールポートで受信したブレーク信号に応答できなくなり、ユーザがrommonにアクセスできなくなる場合があります。この問題は、2019年11月まで製造されたコントローラで、デフォルトのconfig-register設定が0x2102の場合に発生します。この問題は、config-registerを0x2002に設定すると回避できます。この問題は、Cisco Catalyst 9800-LワイヤレスコントローラのROMmon 16.12(3r)で修正されています。ROMMONをアップグレードする方法については、『Cisco Catalyst 9800シリーズワイヤレスコントローラのField Programmable Hardware Devicesのアップグレード』ドキュメントの「Cisco Catalyst 9800-Lワイヤレスコントローラの ROMMONのアップグレード」セクションを参照してください。

- リブートまたはシステムクラッシュの後にこのエラーメッセージが表示された場合は、トラストポイント証明書を再生成することをお勧めします。

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

新しい自己署名トラストポイント証明書を生成するには、次のコマンドを指定された順序で使用します。

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- コマンドを使用して、モビリティMACアドレスが設定されていることを確認しますwireless mobility mac-address。
- これらのプロトコルは、17.9のサービスポートでサポートされるようになりました。
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - コントローラGUI
  - DNS
  - ファイル転送
  - GNMI
  - HTTP
  - HTTPS
  - [LDAP]
  - CSSMと通信するためのSmart Licensing機能のライセンス

- Netconf
- NetFlow
- NTP
- RADIUS（CoAを含む）
- Restconf
- SNMP
- SSH
- SYSLOG
- TACACS+

- 17.9用のAPイメージは、最初に許可されたAPフラッシュよりも大きいものです。17.9イメージのダウンロード時にAPに十分なスペースがないという苦情が出た場合は、17.3.5までのアップグレードパスがリリースノートで説明されているとおりに守られていなかったか、APで古いAireOSイメージが稼働していることが原因と考えられます。17.3.5以降のWLCを通過するか、AireOSイメージを最新のものにアップグレードすると、APフラッシュのサイズが変更され、17.9イメージのダウンロードが可能になります。
- APを17.12以降のリリースにアップグレードすると、コンソールボーレートはすぐには変更されません。ただし、工場出荷時の初期状態にリセットした場合（または新しいAPが17.12以降のWLCに加入した場合）、デフォルトでは115200コンソールボーレートが使用されます。

ダウングレード

ダウングレードは公式にはサポートされておらず、新しい機能の設定が失われる可能性があります。ただし、実際にはダウングレードが発生する可能性があるため、このドキュメントでは、ダウングレードを回避するための最も一般的なトラップのリストを示します。必要な情報を見つけるには、ダウングレード元のバージョン（ダウングレード前のバージョン）を確認します。

ジブラルタル

16.12.2

- ここで指摘することは何もありません。

16.12.3

- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。

16.12.4

- このリリースからより低いリリースにダウングレードする場合、Cisco Bug ID CSCvt69990/Cisco Bug ID CSCvv87417によりテレメトリが設定されていると、WLCがブートループに陥る可能性があります。
- Cisco Catalyst 9800ワイヤレスコントローラは、17.xから16.12.4aにダウングレードするとリロードする可能性があります。これを回避するには、Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。

アムステルダム

17.1.1

- このリリースからより低いリリースにダウングレードする場合、Cisco Bug ID CSCvt69990/CSCvv8741が原因でテレメトリが設定されていると、WLCがブートループに陥る可能性があります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。

17.2.1

- このリリースからより低いリリースにダウングレードする場合、Cisco Bug ID CSCvt69990/Cisco Bug ID CSCvv87417によりテレメトリが設定されていると、WLCがブートループに陥る可能性があります。
- Cisco IOS XE Amsterdam 17.3.1から以前のリリースにダウングレードすると、4よりも高い範囲で設定されているポートチャネルが表示されなくなります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。

17.3.1

- このリリースからより低いリリースにダウングレードする場合、Cisco Bug ID CSCvt69990によりテレメトリが設定されていると、WLCがブートループに陥る可能性があります

  /CSCvv8741

- Cisco IOS XE Amsterdam 17.3.1から以前のリリースにダウングレードすると、より高い範囲で設定されているポートチャネルが表示されなくなります。
- Cisco IOS XE Amsterdam 17.3.1からそれ以前のリリースにダウングレードする場合、「wireless country」コマンドを設定しておくと、17.3より前のリリースには存在しなかったので、再度ウィザードに直面する可能性があります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウン

グレードすることを推奨します。
- Cisco IOS XE Amsterdam 17.3.x（ローカルスイッチングIPv6 AVCをサポート）からCisco IOS XE Gibraltar 16.12.x（ローカルスイッチングIPv6 AVCをサポートしない）にダウングレードする場合、WLANポリシープロファイルをシャットダウンすることはできません。このような場合は、既存のWLANポリシープロファイルを削除し、新しいプロファイルを作成することを推奨します。

17.3.2

- Cisco Bug ID CSCvt69990/Cisco Bug ID CSCvv87417によりテレメトリが設定されている場合、このリリースからより低いリリースにダウングレードすると、WLCはブートループに陥ります。
- Cisco IOS XE Amsterdam 17.3.1から以前のリリースにダウングレードすると、より高い範囲で設定されているポートチャネルが表示されなくなります。
- Cisco IOS XE Amsterdam 17.3.1からそれ以前のリリースにダウングレードする場合、「wireless country」コマンドを設定しておくと、17.3より前のリリースには存在しなかったので、再度ウィザードに直面する可能性があります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。
- Cisco IOS XE Amsterdam 17.3.x（ローカルスイッチングIPv6 AVCをサポート）からCisco IOS XE Gibraltar 16.12.x（ローカルスイッチングIPv6 AVCをサポートしない）にダウングレードする場合、WLANポリシープロファイルをシャットダウンすることはできません。このような場合は、既存のWLANポリシープロファイルを削除し、新しいプロファイルを作成することを推奨します。

17.3.3

- このリリースからより低いリリースにダウングレードする場合、Cisco Bug ID CSCvt69990/Cisco Bug ID CSCvv87417によりテレメトリが設定されていると、WLCがブートループに陥る可能性があります。
- Cisco IOS XE Amsterdam 17.3.1から以前のリリースにダウングレードすると、より高い範囲で設定されているポートチャネルが表示されなくなります。
- Cisco IOS XE Amsterdam 17.3.1からそれ以前のリリースにダウングレードする場合、「wireless country」コマンドを設定しておくと、17.3より前のリリースには存在しなかったので、再度ウィザードに直面する可能性があります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。
- Cisco IOS XE Amsterdam 17.3.x（ローカルスイッチングIPv6 AVCをサポート）からCisco IOS XE Gibraltar 16.12.x（ローカルスイッチングIPv6 AVCをサポートしない）にダウングレードする場合、WLANポリシープロファイルをシャットダウンすることはできません。このような場合は、既存のWLANポリシープロファイルを削除し、新しいプロファイルを作成することを推奨します。

17.4.1

- Cisco IOS XE Amsterdam 17.4.1から17.3より前のリリースにダウングレードする場合、17.3より前には存在しなかったため、「wireless country」コマンドを設定すると、再びday-0 wizardが発生する可能性があります。
- Cisco IOS XE Amsterdam 17.4.1から以前のリリースにダウングレードすると、17.4が以前のバージョンでサポートされていないコマンドを使用する名前付きテレメトリ宛先を使用するため、テレメトリ接続が失われます。テレメトリ接続を再作成する必要があります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。

17.5.1

- Cisco IOS XE Amsterdam 17.4.1から17.3より前のリリースにダウングレードする場合、17.3より前には存在しなかったため、「wireless country」コマンドを設定すると、再びday-0 wizardが発生する可能性があります。
- Cisco IOS XE Amsterdam 17.4.1から以前のリリースにダウングレードすると、17.4が以前のバージョンでサポートされていないコマンドを使用する名前付きテレメトリ宛先を使用するため、テレメトリ接続が失われます。テレメトリ接続を再作成する必要があります。
- Cisco Catalyst 9800ワイヤレスコントローラを17.xから16.12.4aにダウングレードすると、連続的なリロードが発生します。Cisco IOS XE Gibraltar 16.12.4aではなく16.12.5にダウングレードすることを推奨します。

17.9.x

- 802.1xパスワードは暗号化されているため、このリリースではクリアテキストで表示されません。暗号化されたパスワードをサポートしていない以前のイメージにダウングレードすると、APがスタックし、クレデンシャルが正しくないためにdot1x認証が繰り返し失敗します。クリアテキストのパスワードを設定する前にAPがコントローラに加入できるようにするには、APスイッチポートで802.1xを無効にする必要があります。

17.10.1

- 802.1xパスワードは暗号化されているため、このリリースではクリアテキストで表示されません。暗号化されたパスワードをサポートしていない以前のイメージにダウングレードすると、APがスタックし、クレデンシャルが正しくないためにdot1x認証が繰り返し失敗します。クリアテキストのパスワードを設定する前にAPがコントローラに加入できるようにするには、APスイッチポートで802.1xを無効にする必要があります。

17.11.1

- 802.1xパスワードは暗号化されているため、このリリースではクリアテキストで表示されません。暗号化されたパスワードをサポートしていない以前のイメージにダウングレードすると、APがスタックし、クレデンシャルが正しくないためにdot1x認証が繰り返し失敗します。クリアテキストのパスワードを設定する前にAPがコントローラに加入できるようにするには、APスイッチポートで802.1xを無効にする必要があります。

17.12.x

- 802.1xパスワードは暗号化されているため、このリリースではクリアテキストで表示されません。暗号化されたパスワードをサポートしていない以前のイメージにダウングレードすると、APがスタックし、クレデンシャルが正しくないためにdot1x認証が繰り返し失敗します。クリアテキストのパスワードを設定する前にAPがコントローラに加入できるようにするには、APスイッチポートで802.1xを無効にする必要があります。

関連情報

- 17.1ホットパッチおよびローリングAPアップグレードガイド
- 17.3ホットパッチおよびISSUアップグレードガイド
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。