# Cisco Application Policy Infrastructure Controller エンタープライズ モジュール リリース 1.4.x アップグレード ガイド

**初版**：2016 年 05 月 26 日

**最終更新**：2017 年 02 月 20 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

# 目 次


はじめに v

対象読者 v

表記法 v

関連資料 vii

マニュアルの入手方法およびテクニカル サポート ix

はじめる前に 1

サポートされているアップグレード パスの確認 1

アップグレードにかかる時間の確認 2

使用可能な Cisco APIC-EM ポートの確認 2

Cisco APIC-EM のセキュリティ保護 5

コントローラのデータベースとファイルのバックアップ 7

ユーザの認証タイムアウト値の設定 8

Cisco APIC-EM 展開のアップグレード 11

GUI による Cisco APIC-EMのアップグレード 11

CLI による Cisco APIC-EMのアップグレード 15

アップグレード プロセスの確認 17

Cisco APIC-EM アプリケーションのインストール 18

アップグレードの失敗からの回復 21

アップグレードの失敗 21

アップグレードの失敗のサポート ファイルの作成 29

# はじめに


- 対象読者，v ページ
- 表記法，v ページ
- 関連資料，vii ページ
- マニュアルの入手方法およびテクニカル サポート，ix ページ


## 対象読者

このマニュアルは、ネットワーク内の Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（Cisco APIC-EM）をアップグレードする経験豊富なネットワーク管理者を対象としています。このマニュアルを使用して、Cisco APIC-EMの現在のバージョンをアップグレードしてください。

Cisco APIC-EMのインストールの詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*』を参照してください。

コントローラの GUI を初めて使用する場合は、『*Cisco APIC-EM Quick Start Guide*』を参照してください。

（注） Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（Cisco APIC-EM）は、このアップグレード ガイドでは コントローラ とも呼ばれます。

## 表記法

このマニュアルでは、次の表記法を使用しています。

| 表記法 | 説明 |
|---|---|
| ^ または Ctrl | ^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。 |
| **太字** | コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。 |
| *Italic* フォント | 文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。 |
| `courier` フォント | システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。 |
| **`太字の courier`** フォント | ユーザが入力したテキストは、太字の courier フォントで示しています。 |
| [x] | 角カッコの中の要素は、省略可能です。 |
| ... | 構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。 |
| \| | パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。 |
| [x \| y] | どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。 |
| {x \| y} | どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。 |
| [x {y \| z}] | 角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。 |
| string | 引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。 |
| < > | パスワードのように出力されない文字は、山カッコで囲んで示しています。 |
| [ ] | システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。 |

| 表記法 | 説明 |
|---|---|
| !、# | コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。 |

### 読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保管しておいてください。

# 関連資料

この項では、Cisco APIC-EMおよび関連ドキュメントの一覧を示します。これらのドキュメントは、Cisco.com の次に示す URL で入手できます。

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html [英語]

- Cisco APIC-EMのドキュメンテーション：
  - *Cisco Application Policy Infrastructure Controller* エンタープライズ モジュールのリリースノート

- *Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール対応のプラットフォーム
- *Cisco APIC-EM* クイック スタート ガイド（コントローラの GUI から直接アクセス可能）
- *Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール インストレーション ガイド
- *Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール アップグレード ガイド
- *Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイド
- *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
- *Open Source Used In Cisco APIC-EM*

- Cisco APIC-EM向けシスコ ネットワーク可視性アプリケーション
  - *APIC-EM* 向けシスコ ネットワーク可視性アプリケーションのリリース ノート
  - *APIC-EM* 向けシスコ ネットワーク可視性アプリケーション対応のプラットフォーム
  - *APIC-EM* 向けシスコ ネットワーク可視性アプリケーションのユーザ ガイド
- Cisco APIC-EM向けシスコ パス トレース アプリケーション
  - *APIC-EM* 向けシスコ パス トレース アプリケーションのリリース ノート
  - *APIC-EM* 向けシスコ パス トレース アプリケーション対応のプラットフォーム
  - *APIC-EM* 向けシスコ パス トレース アプリケーションのユーザ ガイド
- Cisco APIC-EM向け Cisco EasyQoS アプリケーション
  - *APIC-EM* 向けシスコ パス トレース アプリケーションのリリース ノート
  - *APIC-EM* 向け *Cisco EasyQoS* アプリケーション対応のプラットフォーム
  - *APIC-EM* 向け *Cisco EasyQoS* アプリケーションのユーザ ガイド
- Cisco APIC-EM用 Cisco IWAN のドキュメンテーション：
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network* アプリケーション（*Cisco IWAN App*）
  - *Configuration Guide for Cisco IWAN on Cisco APIC-EM*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco APIC-EM用シスコ ネットワーク プラグ アンド プレイのドキュメンテーション：
  - *Release Notes for Cisco Network Plug and Play*

- *Solution Guide for Cisco Network Plug and Play*
- *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
- *Cisco Open Plug-n-Play Agent Configuration Guide*
- *Mobile Application User Guide for Cisco Network Plug and Play*

（注） ノースバウンド REST API によってコントローラと連携する独自のアプリケーションの開発については、developer.cisco.com/site/apic-em の Web サイトを参照してください。

# マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受け取るには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

# はじめる前に

アップグレードを開始する前に、次の情報をよくお読みください。


- サポートされているアップグレード パスの確認，1 ページ
- アップグレードにかかる時間の確認，2 ページ
- 使用可能な Cisco APIC-EM ポートの確認，2 ページ
- Cisco APIC-EM のセキュリティ保護，5 ページ
- コントローラのデータベースとファイルのバックアップ，7 ページ
- ユーザの認証タイムアウト値の設定，8 ページ


## サポートされているアップグレード パスの確認

次のリリースはすべて、Cisco APIC-EMリリース 1.4.0.x に直接アップグレードできます。

（注） Cisco APIC-EM リリース 1.4.0.x は、VLAN の終端とネットワーク インターフェイス カード（NIC）のボンディングをサポートしていません。これらの機能がある Cisco APIC-EM リリース 1.3.3.x を使用している場合、リリース 1.4.0.x にアップグレードできません。

- 1.3.3.126
- 1.3.2.37
- 1.3.1.9
- 1.3.0.4383

上記の Cisco APIC-EMリリースよりも前のバージョンを使用している場合は、最新のパッチを使用して上記のいずれかのリリースにアップグレードしてから、リリース 1.4.0.x にアップグレードしてください。

# アップグレードにかかる時間の確認

Cisco APIC-EMのアップグレード プロセスは、完了するまでに約 60 分かかる場合があります。アップグレードにかかる実際の時間は、ネットワーク展開の規模、関連するエンドポイントの数、使用中のアプリケーション（EasyQoS、IWAN、Network Plug and Play）など、いくつかの要因に左右されます。

（注） アップグレード プロセスではサービスがそれぞれ異なるタイミングで再起動するので、すべてのアプリケーションが同時に起動することはありません。

重要 Cisco APIC-EMコントローラはアップグレード プロセス中は操作不可能になるため、ネットワークのオフピーク時またはメンテナンス期間中にアップグレードをスケジューリングすることをお勧めします。

# 使用可能な Cisco APIC-EM ポートの確認

次の表に、着信トラフィックを許可する Cisco APIC-EMポートと、発信トラフィックに使用されるCisco APIC-EM ポートを示します。コントローラでこれらのポートが着信および発信の両方のトラフィック フローに対して開かれていることを確認する必要があります。

次の表に、コントローラへの着信トラフィックを許可する Cisco APIC-EM ポートを示します。

**表 *1*：*Cisco APIC-EM*着信トラフィック ポートのリファレンス**

| ポート番号 | 許可されるトラフィック | プロトコル（**TCP** または **UDP**） |
|---|---|---|
| 22 | SSH | TCP |
| 80 | HTTP | TCP |
| 123 | NTP | UDP |
| 162 | SNMP | UDP |
| 443 | HTTPS | TCP |

| ポート番号 | 許可されるトラフィック | プロトコル（TCP または UDP） |
|---|---|---|
| 500 | ISAKMP<br>特定の展開でファイアウォールを越えて複数のホストを展開するには、IPSec ISAKMP（Internet Security Association and Key Management Protocol）UDP ポート 500 の通過を許可する必要があります。 | UDP |
| 16026 | SCEP | TCP |

次の表に、コントローラからの発信トラフィックに使用される Cisco APIC-EM ポートを示します。

**表 *2*：*Cisco APIC-EM*発信トラフィック ポートのリファレンス**

| Port Number | 許可されるトラフィック | プロトコル（TCP または UDP） |
|---|---|---|
| 22 | SSH（ネットワーク デバイスへ） | TCP |
| 23 | Telnet（ネットワーク デバイスへ） | TCP |
| 53 | DNS | UDP |

| Port Number | 許可されるトラフィック | プロトコル（TCP または UDP） |
|---|---|---|
| 80 | ポート 80 は出力プロキシ設定に使用できます。<br>さらに、プロキシが Cisco APIC-EM 設定ウィザードで設定されている場合は、8080 など、その他の共通ポートも使用できます（プロキシがすでにネットワークで使用されている場合）。<br>（注） シスコがサポートしている証明書および trustpool にアクセスするには、コントローラから Cisco アドレス（次の URL を参照）への発信 IP トラフィックを許可するようにネットワークを設定します。<br>http://www.cisco.com/security/pki/ | TCP |
| 123 | NTP | UDP |
| 161 | SNMP エージェント | UDP |
| 443 | HTTPS | TCP |
| 500 | ISAKMP<br>特定の展開でファイアウォールを越えて複数のホストを展開するには、IPSec ISAKMP（Internet Security Association and Key Management Protocol）UDP ポート 500 の通過を許可する必要があります。 | UDP |

# Cisco APIC-EM のセキュリティ保護

Cisco APIC-EMは、コントローラがモニタ。・制御するホストとネットワーク デバイスに加えてコントローラ自体にも多くのセキュリティ機能を提供します。コントローラを導入する際は、次のセキュリティに関する推奨事項に従うよう強く推奨されます。

**表 *3*：*Cisco APIC-EM* セキュリティに関する推奨事項**

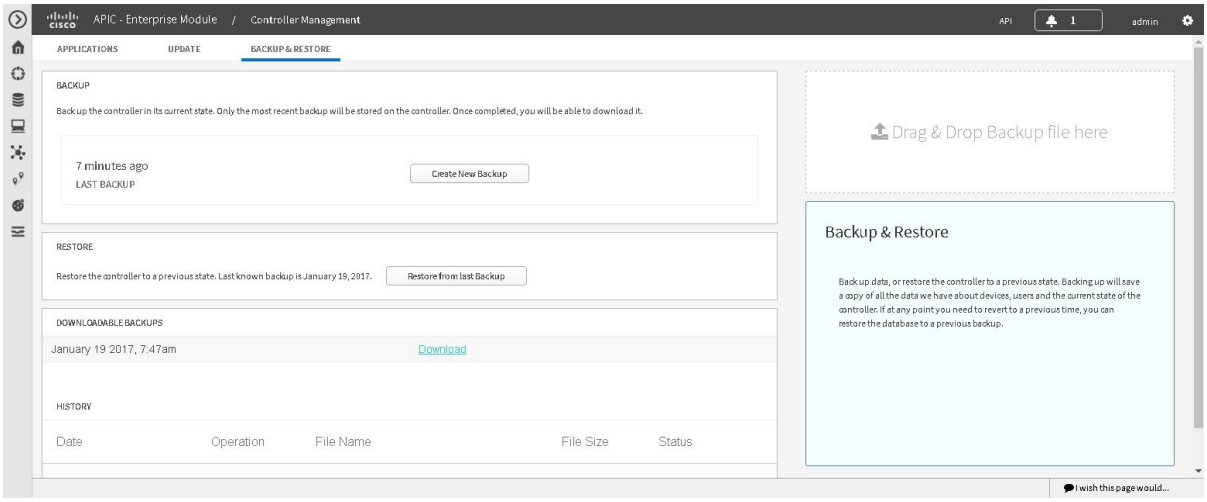
| セキュリティに関する推奨事項 | 参照先 |
|---|---|
| インターネットなどの信頼されていないネットワークにコントローラの管理ポート（たとえばポート22）を開かないよう、ファイアウォールの背後にコントローラを導入します。 | 主要なコントローラ ポートに関する情報については、前の項を参照してください。 |
| マルチホスト設定のホスト間の通信用に IPSec トンネリングを設定します。 | IPSec トンネリングの設定に関する情報については、*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイドのセキュリティに関する章「マルチホスト通信への IPSec トンネリングの設定」を参照してください。 |
| Cisco APIC-EMHTTPS サービスで、TLS 1.0（現在のデフォルト）ではなく、TLS 1.1 または TLS 1.2 を使用するように設定します。TLS 1.2 が推奨されます。ただし、1.0 より後の TLS バージョンを選択する場合は、事前にデバイスが TLS 1.1 や TLS 1.2 もサポートするか確認してください（特に、デバイスがCisco APIC-EMPnP アプリケーションを使用するネットワークに導入される場合）。また、コントローラ UI にアクセスするブラウザなどを含む NB API コンシューマすべてが、TLS 1.1 または TLS 1.2 で通信できることを確認してください。Cisco APIC-EMがサポートするすべてのブラウザ クライアントは、すでに TLS 1.1 以上をサポートしています。 | TLS バージョンの設定に関する情報については、*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイドのセキュリティに関する章「CLI を使用した TLS バージョンの設定」を参照してください。 |

| セキュリティに関する推奨事項 | 参照先 |
|---|---|
| コントローラからの自己署名サーバ証明書を、既知の認証局が署名した証明書に置き換えます。 | このセキュリティに関する推奨事項については、次のいずれかを実行します。<br>• コントローラの証明書のインポートと使用に関する情報については、『*Cisco Application Policy Infrastructure Controller* エンタープライズモジュール管理者ガイド』の設定に関する章「Importing a Certificate」を参照してください。<br>• コントローラの Trustpool のインポートと使用に関する情報については、『*Cisco Application Policy Infrastructure Controller* エンタープライズモジュール管理者ガイド』の設定に関する章「Importing a Trustpool bundle」を参照してください。 |
| モニタおよび管理するコントローラとネットワーク デバイス間に、プロキシ ゲートウェイを設定します。 | コントローラのプロキシゲートウェイの証明書のインポートと使用に関する情報については、『*Cisco Application Policy Infrastructure Controller* エンタープライズモジュール管理者ガイド』の設定に関する章「Importing a Proxy Gateway Certificate」を参照してください。 |
| コントローラの検出機能を使用する場合、ネットワーク デバイスの認証とプライバシーが有効な状態で SNMPv3 を使用します。 | コントローラの SNMPv3 の設定に関する情報については、『*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイド』の設定に関する章「Configuring SNMP」を参照してください。 |

# コントローラのデータベースとファイルのバックアップ

アップグレードを実行する前に、GUI の [Backup & Restore]ウィンドウ使用して、コントローラのデータベースとファイルをバックアップする必要があります。

**図 *1*：*[Backup & Restore]* ウィンドウ**




（注） マルチホスト クラスタでは、データベースとファイルは 3 つのホスト間で複製されて共有されます。マルチホスト クラスタでバックアップと復元を実行する場合は、クラスタ内の 3 つのホストのいずれか1つをバックアップする必要があります。バックアップと復元の詳細については、『*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイド』を参照してください。

## はじめる前に

管理者（ROLE_ADMIN）権限、およびすべてのリソースに対するアクセス権限（[RBAC Scope] が [ALL] に設定されている）、またはグループ化するすべてのリソースを含む RBAC 範囲に対するアクセス権限をもっている必要があります。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースに対するアクセス権限をもっている必要があります（カスタム RBAC 範囲がグループ化するすべてのリソースに設定されている）。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限の詳細については、『*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイド』の「*Managing Users and Roles*」の章を参照してください。

**ステップ 1** [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

**ステップ 2** ドロップダウン メニューから [App Management]リンクをクリックします。

（注） 以前のバージョンのコントローラ ソフトウェアでは、[Backup and Restore]の機能には [Settings] ナビゲーション ウィンドウから直接アクセスできました。[Backup and Restore]オプションは、[Settings] ナビゲーション ウィンドウにまだ表示されていますが、このリリースでは、この GUI の場所からこの機能にアクセスできません。

**ステップ 3** ウィンドウの一番上にある [Backup and Restore]タブをクリックします。

**ステップ 4** [Backup & Restore]ウィンドウで、[Create New Backup] ボタンをクリックしてバックアップ ファイルを作成します。

[Create New Backup]ボタンをクリックすると、[Backup in Progress] ウィンドウが GUI に表示されます。

この処理中に、Cisco APIC-EMはコントローラのデータベースおよびファイルの圧縮された *.backup* ファイルを作成します。このバックアップ ファイルには日時のタイムスタンプが与えられ、ファイル名に反映されます。使用されるファイル命名規則は *yyyy-mm-dd-hh-min-seconds*（年□月□日□時□秒）です。

次に例を示します。

*backup_2016_08_14-08-35-10*

（注） デフォルトの日時のタイムスタンプの命名規則を使用する代わりに、必要に応じて、バックアップ ファイルの名前を変更できます。

このバックアップ ファイルはコントローラ内のデフォルトの場所に保存されます。バックアップ プロセスが終了すると、[Backup Done!]通知が表示されます。一度に 1 つのバックアップ ファイルのみがコントローラに保存されます。

（注） バックアップ プロセスが何らかの理由で失敗しても、コントローラとデータベースには影響しません。また、バックアップが失敗した理由を示すエラー メッセージが表示されます。バックアップの失敗の最も一般的な原因は、ディスク領域の不足です。バックアップ プロセスに失敗した場合、コントローラに十分なディスク領域があることを確認し、再度バックアップを試みる必要があります。

**ステップ 5** （任意）別の場所にバックアップ ファイルのコピーを作成します。

バックアップが成功すると、[Download]リンクが GUI に表示されます。そのリンクをクリックして、バックアップ ファイルのコピーをダウンロードし、ネットワーク上の安全な場所に保存します。

（注） コントローラのバックアップ ファイルを復元する方法については、『*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイド』を参照してください。

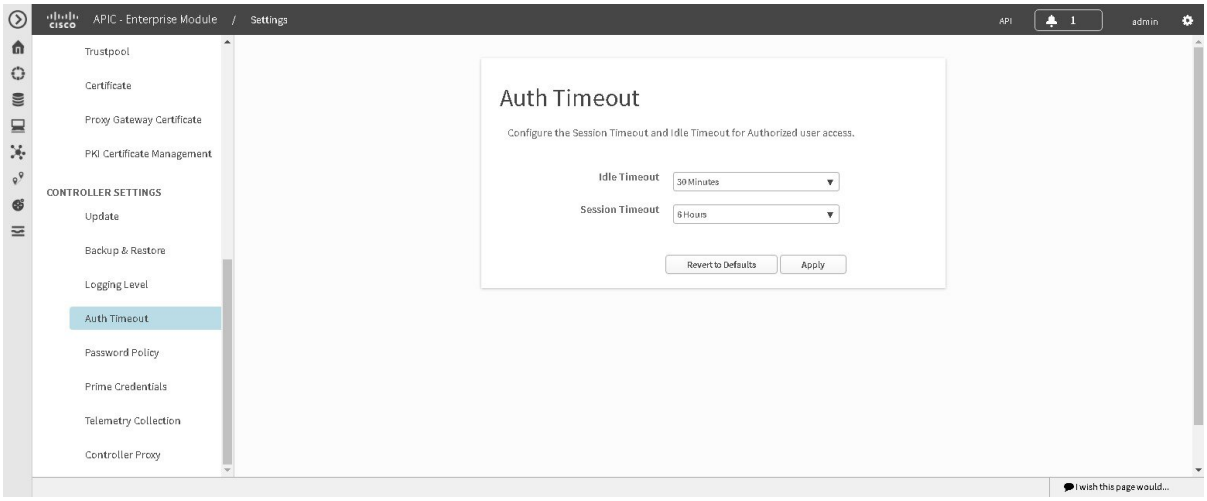
# ユーザの認証タイムアウト値の設定

Cisco APIC-EMの GUI の [Authentication Timeout] ウィンドウを使用して、ユーザがクレデンシャル（ユーザ名とパスワード）を使ってコントローラに再びログインする必要がある認証タイムアウトを設定できます。

Cisco APIC-EMのソフトウェア アップデート プロセスを開始する前に、GUI の [Authentication Timeout]ウィンドウのアイドル タイムアウト値を 1 時間以上に設定することを推奨します。ソフ

トウェア アップデート プロセス中にユーザがアイドル タイムアウトによってログアウトした場合、このプロセスは失敗するため、再度開始する必要があります。

**図 *2*：*[Authenticate Timeout]* ウィンドウ**




## はじめる前に

管理者（ROLE_ADMIN）権限、およびすべてのリソースに対するアクセス権限（[RBAC Scope] が [ALL] に設定されている）、またはグループ化するすべてのリソースを含む RBAC 範囲に対するアクセス権限をもっている必要があります。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースに対するアクセス権限をもっている必要があります（カスタム RBAC 範囲がグループ化するすべてのリソースに設定されている）。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限の詳細については、『*Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール管理者ガイド』の「*Managing Users and Roles*」の章を参照してください。

**ステップ 1** コントローラの GUI の [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

**ステップ 2** ドロップダウン メニューの [Settings]リンクをクリックします。

**ステップ 3** [Settings]ナビゲーション ウィンドウで [Authentication Timeout] をクリックして、[Authentication Timeout] ウィンドウを表示します。

**ステップ 4** [Idle timeout]ドロップダウン メニューを使用して、アイドル タイムアウトの値を設定します。
アイドル タイムアウトは、1 時間を超える値に設定する必要があります。

**ステップ 5** （任意）[Session Timeout]ドロップダウン メニューを使用して、セッション タイムアウトの値を設定します。
セッション タイムアウト値を最大 24 時間まで 30 分単位で設定できます。デフォルト値は 6 時間です。

**ステップ 6** [Apply]ボタンをクリックして、コントローラに設定を適用します。

第 2 章

# Cisco APIC-EM 展開のアップグレード

最新の Cisco APIC-EM バージョンへのアップグレードおよび検証については、この章の以下のセクションを参照してください。


- GUI による Cisco APIC-EMのアップグレード，11 ページ
- CLI による Cisco APIC-EMのアップグレード，15 ページ
- アップグレード プロセスの確認，17 ページ
- Cisco APIC-EM アプリケーションのインストール，18 ページ


# GUI による Cisco APIC-EMのアップグレード

コントローラの GUI アップデート手順を使用してCisco APIC-EMを最新バージョンに更新できます。この手順では、次のタスクを実行する必要があります。

1. シスコの安全なクラウドからリリース アップグレード パックをダウンロードします。
2. リリース アップグレード パックに対しチェックサムを実行します。
3. GUI を使用してコントローラにリリース アップグレード パックをアップロードします。
4. リリース アップグレード パックでコントローラのソフトウェアを更新します。

**重要** この手順とあわせて、Cisco APIC-EMのリリース ノートの最新バージョンも参照してください。そのリリースのアップグレードに固有の追加要件がある可能性があります。この手順を開始する前に、まず『*Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*』を参照してください。

（注） マルチホスト クラスタでは、1 つのホストだけを更新します。その 1 つのホストを更新すると、他の 2 つのホストはリリース アップグレード パックを使用して自動的に更新されます。

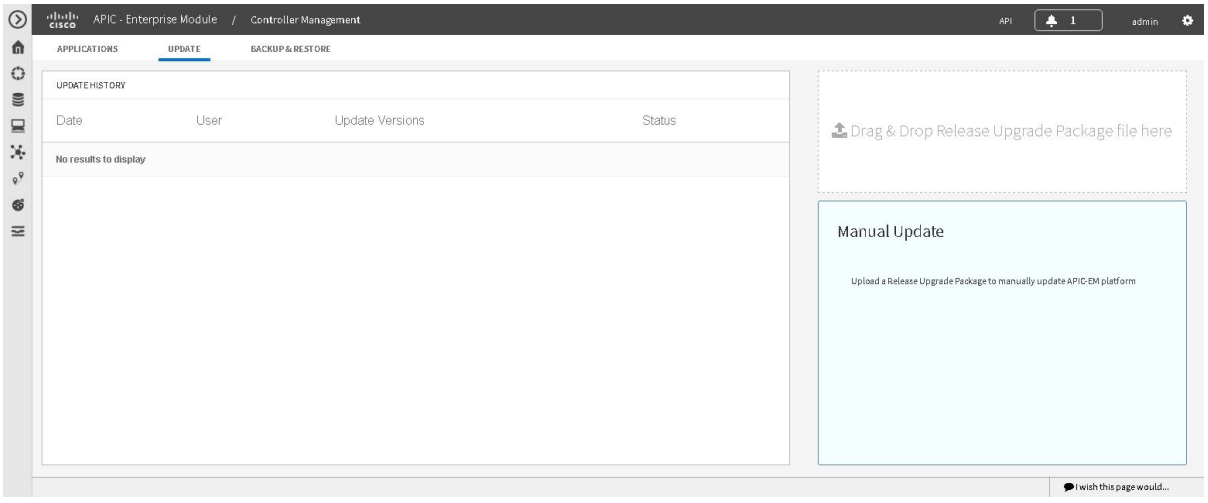
リリースアップグレードパックは圧縮もされているtarファイルとしてダウンロードできるので、リリース アップグレード パックには .tar.gz の拡張子が付いています。リリース アップグレード パック自体は次の更新ファイルの一部またはすべてで構成されます。

- サービス ファイル
- Grapevine ファイル
- Linux ファイル

（注） 各リリースアップグレードパックには、セキュリティのために暗号化されたシスコの署名と、パッケージを検証するリリース バージョンのメタデータが含まれています。

アップロードおよび更新手順は、Cisco APIC-EMGUI の [Update] ウィンドウを使用して実行します。

**図 *3*：*[Update]* ウィンドウ**




（注） アップロードおよびソフトウェア アップデートが正常に完了した後で、以前の Cisco APIC-EM バージョンにロールバックすることはできません。

## はじめる前に

Cisco APIC-EMが正常にインストールされ、動作している必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースに対するアクセス権限（[RBAC Scope] が [ALL] に設定されている）、またはグループ化するすべてのリソースを含む RBAC 範囲に対するアクセス権限をもっている必要があります。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースに対するアクセス権限をもっている必要があります（カスタム RBAC 範囲がグループ化するすべてのリソースに設定されている）。

（注） VMware vSphere 環境内の仮想マシンでCisco APIC-EMを更新またはアップグレードする場合、ESXi ホストの時刻設定も NTP サーバに同期されていることを確認する必要があります。確実に同期されていないと、アップグレードが失敗する原因となります。

安全なシスコ Web サイトで Cisco APIC-EMのソフトウェア アップデートをダウンロード可能であるという通知をシスコから受け取っている必要があります。

Cisco APIC-EMのソフトウェア アップデートの提供について次のように通知されます。

- シスコ サポートからの電子メール通知や最新のリリース ノート。
- コントローラの GUI によるシステム通知。

（注） 使用可能なリリース アップグレード パックに関する通知は、メニュー バーの [System Notifications]アイコンをクリックすると確認できます。

**ステップ 1** Cisco APIC-EMのアップデート ファイルおよびチェックサムに関するシスコ通知の情報を確認します。シスコ通知には、リリース アップグレード パックの場所と、Message Digest 5（MD5）または Secure Hash Algorithm（SHA）512 ビット（SHA512）チェックサム用の検証値が明記されています。

（注） Cisco APIC-EMリリース アップグレード パックは、特定のアップデートの要件に基づいてさまざまなサイズがあるビット ファイルです。リリース アップグレード パックは、数ギガビットの大きさになる可能性があります。

**ステップ 2** リリース アップグレード パックをシスコの安全な Web サイトからラップトップまたはネットワーク内の場所にダウンロードします。

**ステップ 3** 所有しているチェックサム検証ツールまたはユーティリティを使用して（MD5 または SHA512）リリース アップグレード パックに対するチェックサムを実行します。

**ステップ 4** チェックサム検証ツールまたはユーティリティから表示されたチェックサム検証値を確認します。チェックサム検証ツールまたはユーティリティからの出力が、シスコ通知または安全なシスコ Web サイトにある適切なチェックサム値と一致した場合は次のステップに進みます。出力がチェックサム値と一致しない場合、リリース アップグレード パックをダウンロードし、別のチェックサムを実行します。チェックサム検証の問題が解決しなかった場合は、シスコ サポートに連絡してください。

**ステップ 5** [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

**ステップ 6** ドロップダウン メニューから [App Management]リンクをクリックします。

（注） 以前のバージョンのコントローラ ソフトウェアでは、[Update]の機能には[Settings]ナビゲーション ウィンドウから直接アクセスできました。[Update]オプションは [Settings] ナビゲーション ウィンドウにまだ表示されていますが、このリリースでは、この GUI の場所からこの機能にアクセスできません。

**ステップ 7** ウィンドウの一番上にある [Update]タブをクリックします。

**ステップ 8** リリース アップグレード パックがコントローラの更新に使用できる（ステップ 4 でチェックサム値が一致）場合、リリース アップグレード パックをラップトップまたはネットワークのダウンロード場所から[Update]ウィンドウの [Manual Update] フィールドにドラッグ アンド ドロップします。
リリース アップグレード パックを [Manual Update]フィールドにドロップすると、アップロード プロセスが開始されます。

アップロード プロセスはリリース アップグレード パックのサイズとネットワーク接続によっては数分かかることがあります。アップロード プロセス中はコントローラを引き続き使用できます。アップロード プロセスが終了し、更新プロセスが開始されると、コントローラを使用できません。

（注） 何らかの理由で [Update]ウィンドウを閉じると、アップロード プロセスが停止します。アップロード プロセスを再開するには、[Update]ウィンドウを開いて、リリース アップグレード パックを [Manual Update]フィールドに再度ドラッグ アンド ドロップします。アップロード プロセスは以前停止した場所から開始されます。コントローラの使用中にアップロード プロセスが中断されないようにするには、GUI で他のタスクに使用する追加ウィンドウを開きます。アップロード プロセス中は [Update]ウィンドウを開いたままにします。

**ステップ 9** アップロードプロセスが終了すると、更新プロセスが自動的に開始されます。更新プロセスが開始され、処理中であることを示すメッセージが GUI に表示されます。
更新プロセス中はコントローラの使用を中止する必要があります。更新プロセス中に、コントローラがシャットダウンし、再起動する可能性があります。シャットダウンプロセスには数分かかることがあります。

（注） 更新プロセスの開始時に、コントローラはリリース アップグレード パックの 2 番目の検証テストを実行します。リリース アップグレード パック自体に含まれている暗号化されたセキュリティ値（署名）は、コントローラで復号化および確認されます。この2番目の検証テストでは、アップロードされたリリース アップグレード パックがシスコから取得されていることを確認します。リリース アップグレード パックは更新処理に進む前にこの 2 番目の検証テストに合格する必要があります。

**ステップ 10** 更新プロセスが完了すると、成功または失敗の通知を受信します。
更新が成功した場合は更新成功の通知が届き、コントローラの使用を続行できます。更新が失敗した場合は、推奨される是正措置が示された更新失敗の通知が届きます。

更新後（または更新の試行後）は、[Update]ウィンドウの [Update History]フィールドにも関連情報が表示されます。次の更新データがこのフィールドに表示されます。

- [Date]：更新のローカルの日時
- [User]：更新を開始したユーザのユーザ名
- [UpdateVersion]：矢印で示されたリリース アップグレード パックのバージョンの更新パス
- [UpdateStatus]：更新のステータス（成功または失敗）

（注） このフィールドの失敗ステータスにカーソルを合わせると（マウスオーバー）、失敗に関する詳細が表示されます。

# CLI による Cisco APIC-EMのアップグレード

CLI のアップグレード手順では、次のタスクを実行する必要があります。

1. ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトからリリース アップグレード パック（.tar ファイル）をダウンロードします。
2. ファイルに対してチェックサムを実行します。
3. アプライアンス、サーバ、または仮想マシン上の場所にファイルを保存します。
4. ファイルに対して Grapevine アップグレード コマンドを実行します。

### はじめる前に

Cisco APIC-EMが正常にインストールされ、動作している必要があります。

Cisco APIC-EMのソフトウェア アップグレードをセキュアなシスコ Web サイトからダウンロードできるという通知を、シスコから受信している必要があります。

この手順を実行するには、Grapevine への SSH アクセス権限が必要です。

重要 リリースのアップグレードについてさらに要件が追加されている可能性があるため、この手順と併せて、Cisco APIC-EMの最新バージョンのリリース ノートもお読みください。

**ステップ 1** Cisco APIC-EMのアップグレードに関するシスコからの通知で情報を確認します。
シスコからの通知には、リリース アップグレード パックの場所、および Message Digest 5（MD5）または Secure Hash Algorithm（SHA）512 ビット（SHA512）チェックサムの検証値の場所が指定されています。

（注） Cisco APIC-EMリリース アップグレード パックはビット ファイルになっており、特定のアップグレードの要件に応じてサイズが異なります。リリース アップグレード パックは、数ギガビットの大きさになることもあります。

**ステップ 2** ソフトウェア ダウンロード リンクのセキュアなシスコ Web サイトから Cisco APIC-EM のアップグレード パックをダウンロードします。
リリース アップグレード パックは、圧縮された tar ファイルとしてダウンロードできるので、リリース アップグレード パックには .tar.gz 拡張子が付いています。リリース アップグレード パック自体は、次の更新ファイルの一部またはすべてから構成されています。

- サービス ファイル
- Grapevine ファイル
- Linux ファイル

（注） 各リリース アップグレード パックには、セキュリティのために暗号化されたシスコの署名と、パッケージを検証するリリース バージョンのメタデータが含まれています。

**ステップ 3** 所有しているチェックサム検証ツールまたはユーティリティ（MD5 または SHA512）を使用し、ファイルに対してチェックサムを実行します。

**ステップ 4** チェックサム検証ツールまたはユーティリティにより表示されたチェックサム検証値を確認します。チェックサム検証ツールまたはユーティリティの出力が、シスコ通知またはセキュアなシスコ Web サイトの適切なチェックサム値と一致した場合は、次のステップに進みます。出力がチェックサム値と一致しない場合は、リリース アップグレード パックをダウンロードして、別のチェックサムを実行します。チェックサム検証の問題が継続する場合は、シスコ サポートに連絡してください。

**ステップ 5** ラップトップまたは安全なネットワーク上の場所から、コントローラがあるアプライアンス、サーバ、または仮想マシンにファイルをコピーまたは移動します。

**ステップ 6** セキュア シェル（SSH）クライアントを使用し、設定ウィザードで指定した IP アドレスによりホスト（アプライアンス、サーバ、または仮想マシン）にログインします。

**ステップ 7** プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

**ステップ 8** ファイルが格納されているフォルダに移動し、次のコマンドを実行します。

```
$ grape update upload [path-to-upgrade-package]
```

grape update upload コマンドでは、そのファイルを使ってコントローラのアップグレード（アップロードと更新）へと進みます。

アップグレード プロセス全体にわたってコントローラの使用を控える必要があります。アップグレード プロセス中に、コントローラがシャットダウンして再起動する可能性があります。シャットダウン プロセスには数分かかることがあります。パーセント バーにアップロードの進捗状況が表示されます。アップロード プロセスが完了すると、アップロードの完了および更新プロセスの開始についての通知が届きます。

```
Release upgrade package uploaded successfully, Update process started.
task_id: 8507f3f6-1de2-11e6-bf7e-00505695af10
```

（注） 更新プロセスの開始時に、コントローラはリリース アップグレード パックの 2 番目の検証テストを実行します。リリース アップグレード パック自体には暗号化されたセキュリティ値（署名）が含まれており、この値がコントローラで復号化されてレビューされます。この 2 番目の検証テストでは、リリース アップグレード パックがシスコからアップロードされたものであることが確認されます。アップグレード プロセスを続行するには、リリース アップグレード パックがこの 2 番目の検証テストに合格する必要があります。

ヒント grape task display task_id コマンドを使用して、更新タスクの進捗状況をモニタします。通知に示されている更新タスク ID を使用します（上記を参照）。

**ステップ 9** アップグレードプロセス（アップロードと更新）が完了すると、成功または失敗を示す通知が届きます。アップグレードに成功した場合は、アップグレードの成功を示す通知が届き、コントローラの使用を続行できます。アップグレードに失敗した場合は、アップグレードの失敗と推奨是正措置に関する通知が届きます。

### 次の作業

アップグレード プロセスを確認します（アップグレード プロセスの確認, （17 ページ）を参照）。

# アップグレード プロセスの確認

アップグレードが正常に行われたかどうかを確認するには、次のいずれかを実行します。

- コントローラの GUI を確認します。

  更新すると、更新に関する情報が [Update]ウィンドウの [Update History]フィールドにも表示されます。このフィールドには次の更新データが表示されます。

  - [Date]：ローカルな更新日時
  - [User]：更新を開始した人物のユーザ名
  - [UpdateVersion]：リリース アップグレード パックのバージョンの更新パスが矢印で示されます。
  - [UpdateStatus]：更新のステータス（成功または失敗）。

  （注） このフィールドの失敗ステータスの上にカーソルを置くと（マウスオーバー）、その失敗に関する詳細が表示されます。

- セキュア シェル（SSH）クライアントを使用し、設定ウィザードで指定した IP アドレスでホスト（物理または仮想）にログインして、次の CLI コマンドを実行します。

  - grape update history：個々のタスク ID など、コントローラの更新履歴を表示します。
  - grape release display current：現在実行されている Cisco APIC-EM ソフトウェア リリースをサービスおよびバージョンと共に表示します。
  - grape instance display：サービス インスタンスとバージョンを表示します。
  - grape instance status：サービス インスタンスのステータスとバージョンを表示します。

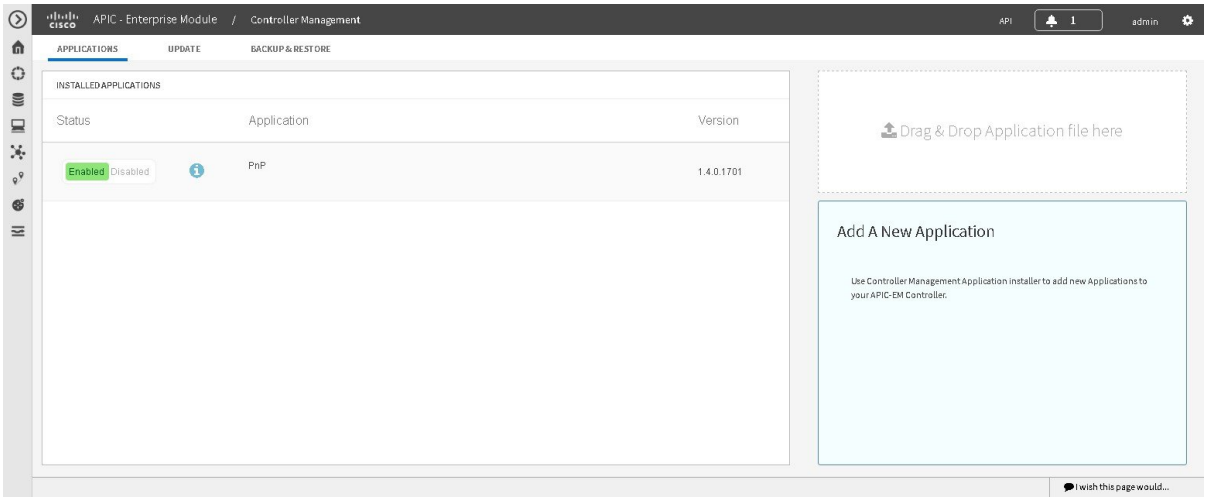
また、ネットワークテスト（ディスカバリやパストレースなど）を実行して、コントローラが期待どおりに機能しているかどうか、およびユーザがネットワークで認証されてリソースにアクセスできるかどうかを確認することを推奨します。

# Cisco APIC-EM アプリケーションのインストール

Cisco IWAN アプリケーションは、Cisco APIC-EMリリース 1.4.0.x の新規インストールには含まれておらず、アップグレードにも含まれていない可能性があります（個々のアップグレード パスに依存します）。

次のように、コントローラの GUI を使用した追加手順で、Cisco IWAN をインストールして有効にする必要があります。アプリケーションのインストール手順は簡単です。シスコが提供するアプリケーション バンドルは、[App Management]の [admin]（設定アイコン）の下にあるブラウザ ウィンドウにドロップする必要があります。

**図 *4*：*[App Management]* ウィンドウ**




追加のアプリケーションをインストールするには、次の手順を実行します。

**重要** Cisco APIC-EMの設定を完了してから、次の手順を実行します。マルチホストの Cisco APIC-EM を設定する場合、マルチホスト設定のすべてのホストのセットアップを完了した上で、この手順を実行します。

## はじめる前に

次の一連の手順のいずれかを実行しました。

- 『*Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*』に記載された手順に従って、Cisco APIC-EM リリース 1.4.0.x をインストールしました。

- このガイドの前の手順で説明されたように、Cisco APIC-EMコントローラ ソフトウェアをバージョン 1.4.0.x にアップグレードしました。

管理者（ROLE_ADMIN）権限、およびすべてのリソースに対するアクセス権限（[RBAC Scope] が [ALL] に設定されている）、またはグループ化するすべてのリソースを含む RBAC 範囲に対するアクセス権限をもっている必要があります。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースに対するアクセス権限をもっている必要があります（カスタム RBAC 範囲がグループ化するすべてのリソースに設定されている）。

Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限と RBAC の範囲の詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*』の「Configuring the Cisco APIC-EM Settings」の章の「User Settings」を参照してください。

**ステップ 1** Cisco.com からアプリケーション バンドルをダウンロードします。
バンドルをラップトップまたはネットワークの安全な場所に保存します。

**ステップ 2** ブラウザのアドレス バーに、次の形式で Cisco APIC-EMの IP アドレスを入力します。
**https://***IP address*

**ステップ 3** 起動ページで、ユーザ名とパスワードを入力します。
APIC-EM コントローラの [Home]ウィンドウが表示されます。

**ステップ 4** [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

**ステップ 5** ドロップダウン メニューから [App Management]リンクをクリックします。

**ステップ 6** ブラウザの [App Management]ウィンドウの専用ドラッグ アンド ドロップ フィールドに、アプリケーション バンドルをドラッグ アンド ドロップします。

（注） このステップで、アプリケーションのインストール プロセスが開始されます。完了するまで数分かかる可能性があります。

**ステップ 7** アプリケーションがアップロードされ、インストールされたら、アプリケーション名の隣にあるスイッチを切り替えて、アプリケーションを有効にします。

### 次の作業

ネットワーク配置で必要な場合、上記のステップを繰り返して他のアプリケーションをアップロード/インストールし、有効にします。

第 3 章

# アップグレードの失敗からの回復


- アップグレードの失敗，21 ページ
- アップグレードの失敗のサポート ファイルの作成，29 ページ


## アップグレードの失敗

次の表は、発生する可能性があるアップグレード エラーとその回復方法の一部を示しています。

表 *4*：アップグレードの失敗

| 症状 | 考えられる原因 | 推奨処置 |
|---|---|---|
| ベアメタル サーバでアップグレードに失敗。 | このリリースのシステム要件を満たしていない状態で、コントローラのアップグレードを試みた。 | 最新のCisco APIC-EMリリースノートにアクセスし、システム要件を確認します。ベアメタルのアップグレードに適した特定のシステム要件を確認してください。<br>次の手順を実行して、再度コントローラのアップグレードを実行します。<br>**1** 必要に応じて、サーバに以前のバージョンのコントローラ ソフトウェアを再インストールします。<br>**2** ネットワークの安全な場所に作成し、保存したバックアップ ファイルから、コントローラのデータベースとファイルを復元します。コントローラのデータベースとファイルのバックアップ, （7 ページ）を参照してください。<br>**3** もう一度アップグレードを試します。<br>引き続き失敗する場合は、シスコのサポートに連絡してください。Cisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*』を参照してください。 |

| 症状 | 考えられる原因 | 推奨処置 |
| --- | --- | --- |
| 仮想マシンでアップグレードに失敗。 | このリリースのシステム要件を満たしていない状態で、コントローラのアップグレードを試みた。 | 最新のCisco APIC-EMリリースノートにアクセスし、システム要件を確認します。VMwareリソースプールの要件を含めて、仮想マシンのアップグレードに適した特定のシステム要件を確認してください。<br>次の手順を実行して、再度コントローラのアップグレードを実行します。<br>1 必要に応じて、仮想マシンに以前のバージョンのコントローラ ソフトウェアを再インストールします。<br>2 ネットワークの安全な場所に作成し、保存したバックアップ ファイルから、コントローラのデータベースとファイルを復元します。コントローラのデータベースとファイルのバックアップ, （7 ページ）を参照してください。<br>3 もう一度アップグレードを試します。<br>引き続き失敗する場合は、シスコのサポートに連絡してください。Cisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*』を参照してください。 |

| 症状 | 考えられる原因 | 推奨処置 |
| --- | --- | --- |
| 仮想マシンでアップグレードに失敗。 | コントローラのエラーメッセージが、NTPサーバに問題があることを示している。 | |

| 症状 | 考えられる原因 | 推奨処置 |
| --- | --- | --- |
| | | VMware vSphere 環境内の仮想マシンでCisco APIC-EMをアップグレードする場合、ESXi ホストの時刻設定も NTP サーバに同期されていることを確認する必要があります。同期を確保できないと、アップグレードに失敗します。<br>次の手順を実行して、再度コントローラのアップグレードを実行します。<br>1 必要に応じて、仮想マシンに以前のバージョンのコントローラ ソフトウェアを再インストールします。<br>2 ネットワークの安全な場所に作成し、保存したバックアップ ファイルから、コントローラのデータベースとファイルを復元します。コントローラのデータベースとファイルのバックアップ, （7 ページ）を参照してください。<br>3 NTP サーバの設定が同期していない場合は、SSH を使用してコントローラにログインし、reset_grapevine コマンドを実行して NTP サーバの設定を更新します。<br>4 もう一度アップグレードを試します。<br>引き続き失敗する場合は、シスコのサポートに連絡してください。<br>reset_grapevine コマンドの使用方法およびCisco TAC の連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module* |

| 症状 | 考えられる原因 | 推奨処置 |
|---|---|---|
| | | *Troubleshooting Guide*』を参照してください。 |

| 症状 | 考えられる原因 | 推奨処置 |
| --- | --- | --- |
| ベア メタル サーバまたは仮想マシンでアップグレードに失敗。 | コントローラ GUI のエラーメッセージが、アップグレード後に Cisco APIC-EM で一部のサービスの起動に失敗したことを示している。 | |

| 症状 | 考えられる原因 | 推奨処置 |
|---|---|---|
| | | 次の手順を実行して、再度コントローラのアップグレードを実行します。<br>**1** 必要に応じて、アプライアンス、サーバ、または仮想マシンに、以前のバージョンのコントローラ ソフトウェアを再インストールします。<br>**2** ネットワークの安全な場所に作成し、保存したバックアップ ファイルから、コントローラのデータベースとファイルを復元します。コントローラのデータベースとファイルのバックアップ, （7 ページ）を参照してください。<br>**3** もう一度アップグレードを試します。<br>引き続き失敗する場合は、次のアクションを実行します。<br>• 可能であれば、コントローラの GUI にログインします。<br>• [System Health]タブでサービスのステータスをみて、失敗したサービスを確認します。<br>• 引き続き、RCA ファイルを作成します（アップグレードの失敗のサポートファイルの作成, （29 ページ）を参照）。<br>• サポートを受けるために、コントローラの GUI に表示されたサービスの失敗に関する情報を含む RCA ファイルを送信します。 |

| 症状 | 考えられる原因 | 推奨処置 |
|---|---|---|
| | | 上記の手順およびCisco TACの連絡先情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*』を参照してください。 |

# アップグレードの失敗のサポート ファイルの作成

根本原因の分析（rca）のサポート ファイルを作成して、Cisco APIC-EMのアップグレードの失敗をトラブルシューティングできます。この rca ファイルは、ログ、コンフィギュレーション ファイル、およびコマンド出力から構成されます。この rca ファイルを作成した後、シスコ サポートに電子メールで送信してサポートを受けることができます。

**ステップ 1** セキュア シェル（SSH）クライアントを使用し、設定ウィザードを使用して指定した IP アドレスでホスト（物理または仮想）にログインします。

（注） SSH クライアントで入力する IP アドレスは、ネットワーク アダプタ用に設定した IP アドレスです。この IP アドレスによって、ホストが外部ネットワークに接続されます。

**ステップ 2** プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

**ステップ 3** ホストのbinディレクトリに移動します。binディレクトリにはgrapevineスクリプトが含まれています。

**ステップ 4** サポート ファイルを作成するには、このディレクトリで rca コマンドを入力します。

```
$ rca
mkdir: created directory '/tmp grapevine-rca-2016-08-05_16-22-20-PM_PDT-0700'

--------------------------------------------------------------------------
RCA package created On Tues August 5 16:22:20 PDT 2016
--------------------------------------------------------------------------
```

rca コマンドにより根本原因分析スクリプトが実行され、ログ ファイル、コンフィギュレーション ファイル、およびコマンド出力を含む tar ファイルが作成されます。

### 次の作業

アップグレード問題の解決のサポートを受けるために、この手順で作成された tar ファイルをシスコ サポートに送信します。

# 索 引


## T

time 2

## あ

アップグレードの失敗 21
アプリケーション 18
　インストール 18

## こ

コントローラのバックアップ 7

## し

システム ログ 29

## そ

ソフトウェア アップデート 11, 15
　CLI 15