Cisco Stealthwatch

CIMC および BIOS ファームウェア アップデート ガイド

目次

はじめに

Cisco Integrated Management Controller（CIMC）は、管理サービス用に C シリーズ UCS（Unified Computing Systems）サーバに組み込まれている独立した管理モジュールです。メインサーバ CPU とは別の専用の ARM ベースのプロセッサが CIMC を実行します。UCS サーバには実行中のバージョンの CIMC が付属しているため、初期インストールは不要です。

このドキュメントでは、次の 1 つ以上を使用して、お使いの UCS C シリーズ M4 または M5 ハードウェアの CIMC および BIOS を更新する手順について説明します。

- 仮想コンソール（ISO ファイル）
- USB デバイス（ISO ファイル）
- Stealthwatch SMC（SWU ファイル）

ISO ファイルは、Cisco Stealthwatch Enterprise ダウンロードおよびライセンスセンターからダウンロードできます。SWU ファイル（M5 ハードウェアのみ）は、Cisco Software Central（https://software.cisco.com）から入手できます。

StealthWatch アプライアンス

この更新は、次の表に示す Stealthwatch アプライアンスの UCS C シリーズ M4（x200）および M5（x210）ハードウェアに適用されます。

> ⚠ すべての物理アプライアンスを必ず更新してください。

M4 ハードウェア（x200 シリーズ）	M5 ハードウェア（x210 シリーズ）
SMC 2220	SMC 2210
FC 4200	RFC 4210
FC 5020 エンジン	--
FC 5020 データベース	--
FC 5200 エンジン	FC 5210 エンジン
FC 5200 データベース	FC 5210 データベース
FS 1200	FS 1210
FS 2200	--
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210

Stealthwatch アプライアンスでサポートされるハードウェアの詳細については、『Stealthwatch ハードウェアおよびソフトウェアバージョンのサポートマトリックス』を参照してください。

> この更新は、Dell アプライアンス（IDRAC Enterprise）には適用されません。

対象読者

このガイドは、Stealthwatch 製品（具体的には C シリーズ UCS M4 および M5 ハードウェア）の更新を担当するネットワーク管理者とその他の担当者を対象としています。

用語

このガイドでは、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべての Stealthwatch 製品に対し「アプライアンス」という用語を使用しています。仮想ホストを確立する方法は複数あるため、「仮想コンソール」という用語を使用します。

はじめる前に

更新プロセスを開始する前に、このガイドを参照してプロセス、および更新を計画するために必要な準備、時間、リソースについて確認してください。具体的には、次の操作を実行できることを確認します。

- CIMC Web インターフェイスへのログイン
- CIMC でのリモート ISO のマウント
- 仮想コンソールへのアクセスと使用
- CIMC を使用したアプライアンスのシャットダウン、起動、再起動
- ハードウェアと RAID のステータスの確認

ブラウザ

以下は、ブラウザアクセスに関連しています。

- **互換性のあるブラウザ**：Stealthwatch は Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。
- ショートカット：ブラウザのショートカットを使用して、いずれかの Stealthwatch アプライアンスの CIMC 管理インターフェイスにアクセスしている場合、更新プロセスの完了後はショートカットが機能しないことがあります。その場合は、ショートカットを一旦削除してから再作成してください。

更新に最適な時間

UCS ハードウェアの CIMC および BIOS を更新するための時間とリソースを計画する際には、次の点を検討してください。

ソフトウェア アップデート ファイル

ソフトウェア アップデート ファイルのダウンロードには時間がかかります。

> 事前に Cisco Stealthwatch Enterprise ダウンロードおよびライセンスセンターから必要な ISO ファイルをダウンロードするか、Cisco Software Central（https://software.cisco.com）から SWU ファイルをダウンロードしてください。

ダウンタイム

更新がインストールされ、CIMC が再起動するため、プロセス全体でダウンタイムが発生します。

ベスト プラクティス

推奨事項は次のとおりです。

M4 ハードウェア

M4 ハードウェアの場合、M4 ハードウェアの仮想コンソールから ISO ファイルを使用することをお勧めします。

USB デバイスの ISO ファイルを使用した更新は、M4 ハードウェアでは次善の選択肢です。

M5 ハードウェア

SMC を介して SWU を使用して M5 ハードウェアを更新することを推奨します。

プロセスの概要

更新を成功させ、データ損失を最小限に抑えるためには、順番に手順を実行する必要があります。

⚠ すべての物理アプライアンスを必ず更新してください。

1. 更新ファイルのダウンロード
2. 次のいずれかの方法で CIMC および BIOS を更新します。

更新方法	詳細	注意
仮想コンソールを介した ISO ファイルの使用	M4 ハードウェアで推奨	M4 ハードウェアでは、仮想コンソールを介した ISO ファイルを使用する更新が推奨されます。
SMC を介した SWU ファイルの使用（M5 ハードウェアのみ）	M5 ハードウェアに推奨	M5 ハードウェアでは、SMC を介した SWU ファイルを使用する更新が推奨されます。
USB デバイスでの ISO ファイルの使用	オプション	USB デバイスの ISO ファイルを使用した更新は次善の選択肢です。

3. 更新の成功の確認

更新ファイルのダウンロード

Cisco Stealthwatch ダウンロードおよびライセンスセンター

次の手順に従って、必要な ISO ファイルをダウンロードします。

1. https://stealthwatch.flexnetoperations.com に移動します。
2. Cisco Stealthwatch Enterprise ダウンロードおよびライセンスセンターにログインします。
3. [ダウンロード(Downloads)] > [Stealthwatch のパッチ適用(Patch Stealthwatch)] の順に選択します。
4. [現在のバージョン(Current Versions)] タブで、アプライアンス名をクリックします。ソフトウェアリリースリンクをクリックしてダウンロードします(または [FTPのダウンロード(FTP Download)] を選択します)。
   - [ISO]:ISO ファイルをダウンロードします。
   - 詳細:各項目の横にある下向き矢印をクリックして、追加のソフトウェア情報を表示します。

Cisco Software Central

SMC を介して M5 ハードウェアのみを更新する場合は、次の手順を使用して update-common-SW7VM5-FIRMWARE-01.swu ファイルをダウンロードします。

ファイルをダウンロードするには、次の手順を実行します。

1. シスコ ソフトウェア セントラル(https://software.cisco.com)に移動します。
2. [ダウンロードとアップグレード(Download and Upgrade)] セクションで、[ソフトウェアのダウンロード(Software Download)] を選択します。
3. [製品の選択(Select a Product)] フィールドに **Stealthwatch** と入力します。Enter キーを押します。
4. 該当するアプライアンスモデルを選択します。
5. [ソフトウェアタイプの選択(Select a Software Type)] の下にある [Stealthwatch パッチ(Stealthwatch Patches)] を選択します。
6. update-common-SW7VM5-FIRMWARE-01.swu ファイルをダウンロードし、任意の場所に保存します。

SMC を介した SWU ファイルの使用（M5 ハードウェアのみ）

update-common-SW7VM5-FIRMWARE-01.swu ファイルを使用して、SMC を介して M5 ハードウェアの CIMC および BIOS ファームウェアを更新します。

> ⚠ この SWU ファイルは M5 ハードウェアのみを更新し、Stealthwatch v7.3.0 以降にのみインストールできます。

パッチ更新ファイルをインストールするには、次の手順を実行します。

1. SMC にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックし、[中央管理（Central Management）] をクリックします。
3. [アップデートマネージャ（Update Manager）] をクリックします。
4. [アップデートマネージャ（Update Manager）] ページで [アップロード（Upload）] をクリックし、保存したパッチ更新ファイル（update-common-SW7VM5-FIRMWARE-01.swu）を開きます。
5. アプライアンスの [アクション（Actions）] メニュー、[更新をインストール（Install Update）] の順にクリックします。

> ℹ update-common-SW7VM5-FIRMWARE-01.swu ファイルは、Cisco Software Central（https://software.cisco.com）からダウンロードできます。

仮想コンソールを介した ISO ファイルの使用

ISO ファイルを使用して、仮想コンソールから CIMC と BIOS を更新します。

- M4 ハードウェア（仮想コンソール）：UCS M4 ハードウェアの ISO をマウントすることで CIMC および BIOS を更新する方法については、「**M4 ハードウェア（仮想コンソール）**」を参照してください。
- M5 ハードウェア（仮想コンソール）：UCS M5 ハードウェアの ISO をマウントすることで CIMC および BIOS を更新する方法については、「**M5 ハードウェア（仮想コンソール）**」を参照してください。

更新する必要がある Stealthwatch アプライアンスを確認するには、「**StealthWatch アプライアンス**」を参照してください。すべての物理アプライアンスを必ず更新してください。

> 仮想ホストを確立する方法は複数あるため、「仮想コンソール」という用語を使用します。説明と例では KVM コンソールを使用します。

ISO ファイル

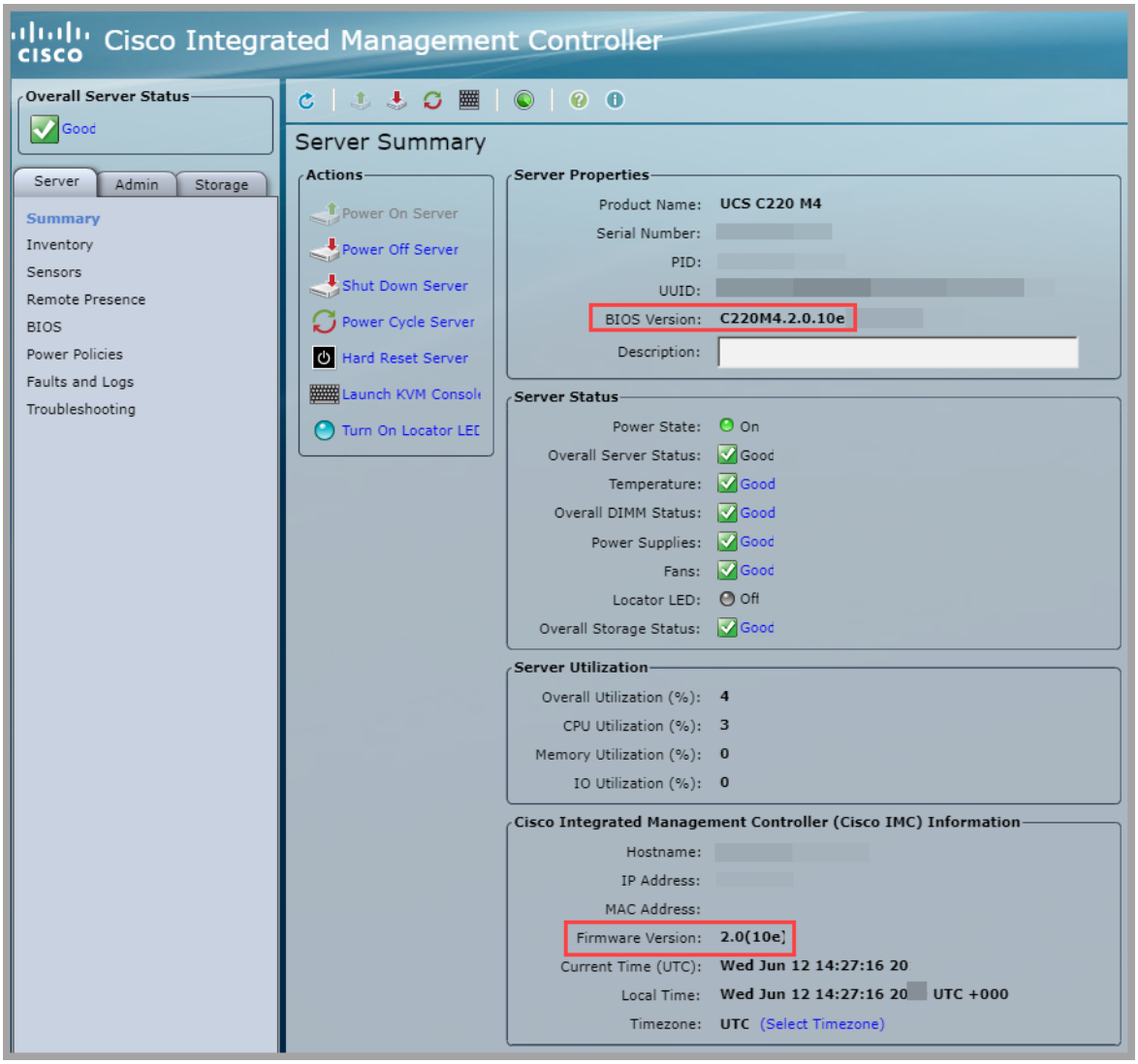
ISO ファイルは、Cisco Stealthwatch Enterprise ダウンロードおよびライセンスセンターからダウンロードできます。

M4 ハードウェア（仮想コンソール）

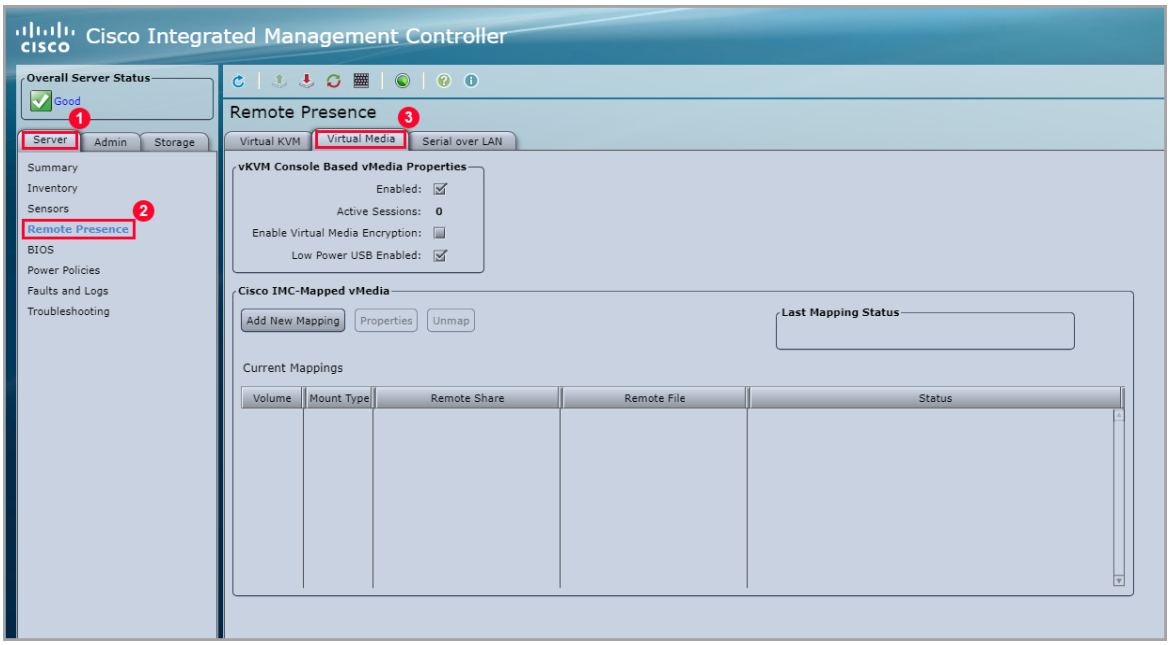
UCS M4 ハードウェアの CIMC および BIOS を更新するには、次の手順を実行します。

1. CIMC にログインします。
2. **BIOS バージョン**と**ファームウェアバージョン**をメモします。

   これらは、更新プログラムが正常にインストールされると変更されます。



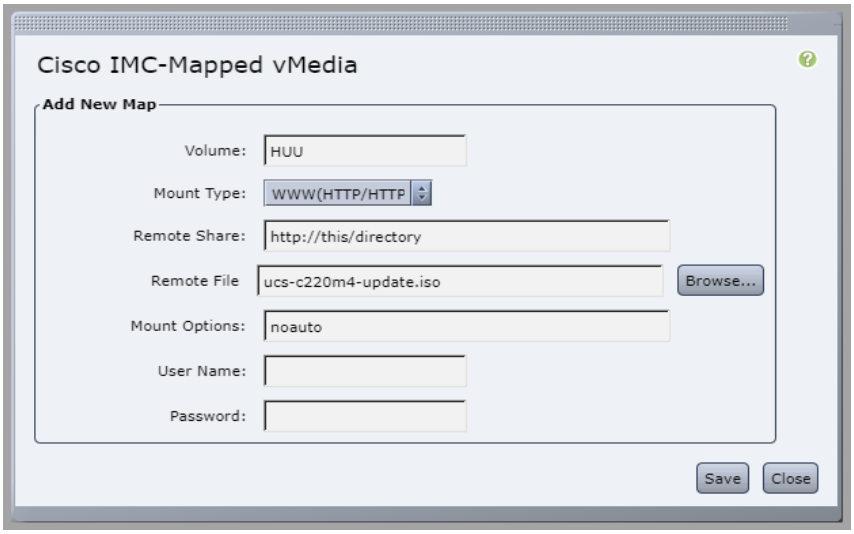
3. ［サーバ（Server）］タブを選択し、［リモートプレゼンス（Remote Presence）］を選択します。
4. ［仮想メディア（Virtual Media）］タブをクリックします。



すでにマッピングされている別のファイルがある場合は、[マップ解除(Unmap)]と[削除(Delete)]をクリックしてそのファイルを削除し、新しい ISO ファイルをロードできるようにします。

5. [新しいマッピングの追加(Add New Mapping)]をクリックします。

   [新しいマッピングの追加(Add New Mapping)]ダイアログボックスが表示されます。

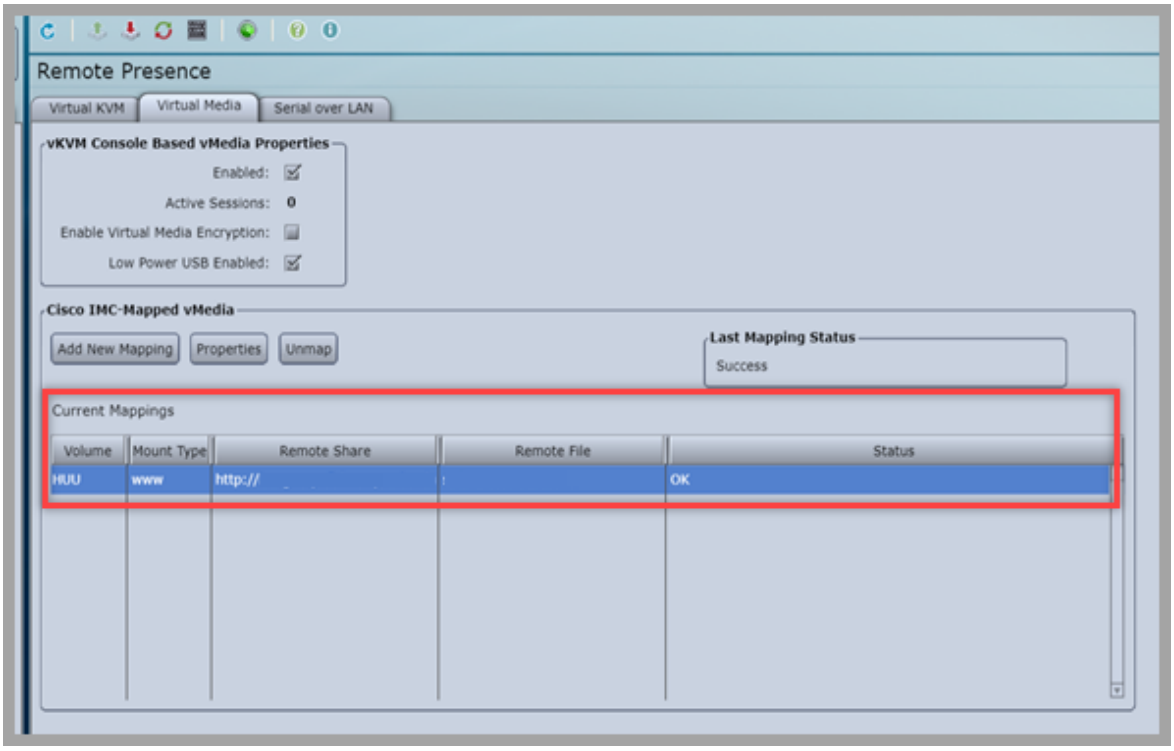


6. 次のフィールドに入力します。
   - [ボリューム(Volume)]フィールドに HUU と入力します。
   - [マウントタイプ(Mount Type)]フィールドで[WWW(HTTP/HTTPS)]を選択します。

> 別のマウントタイプを選択する場合は、対応する通信ポートが有効になっていることを確認してください。

- [リモート共有(Remote Share)]フィールドに ISO ファイルのファイル共有パスを入力します。
  例:**http://this/directory**
- リモートファイルを選択します。
  例:**ucs-c220m4-update.iso**
- [マウントオプション(Mount Options)]フィールドで[noauto]を選択します。
- 要求された場合は、[ユーザ名(User Name)]と[パスワード(Password)]を入力します。

7. [保存(Save)]をクリックします。
8. [現在のマッピング(Current Mappings)]セクションを探し、[ステータス(Status)]列に[OK]と表示されていることを確認します。



9. [変更の保存(Save Changes)]をクリックします。
10. ツールバーの[KVMコンソールを起動(Launch KVM Console])]アイコンをクリックします。

[仮想コンソール（Virtual Console）] ダイアログボックスが表示されます。

11. [電源（Power）] を選択し、[システムのリセット（ウォーム ブート）（Reset System（Warm Boot））] を選択します。

    リブートプロセスが開始されます。

12. リブートプロセス中にブートメニューで F6 を選択します。

    [ブートデバイスを選択してください（Please Select Boot Device）] ダイアログボックスが表示されます。

13. [Cisco CIMC-Mapped vDVD1.22] を選択します。

    [シスコソフトウェアライセンス契約書（Cisco Software License Agreement）] ダイアログボックスが表示されます。

14. [同意します（I Agree）] をクリックします。

    [ファームウェアユーティリティの更新（Firmware Utility Update）] ダイアログボックスが表示されます。

15. [すべて更新&アクティブ化（Update & Activate All）] を選択します。
16. 画面に表示される指示に従って、更新を続行します。

    [ステータス（Status）] は [完了（Completed）] になるまで [進行中（In Progress）] と表示されます。これは時間がかかる場合があります。

    CIMC が更新され、再起動します。

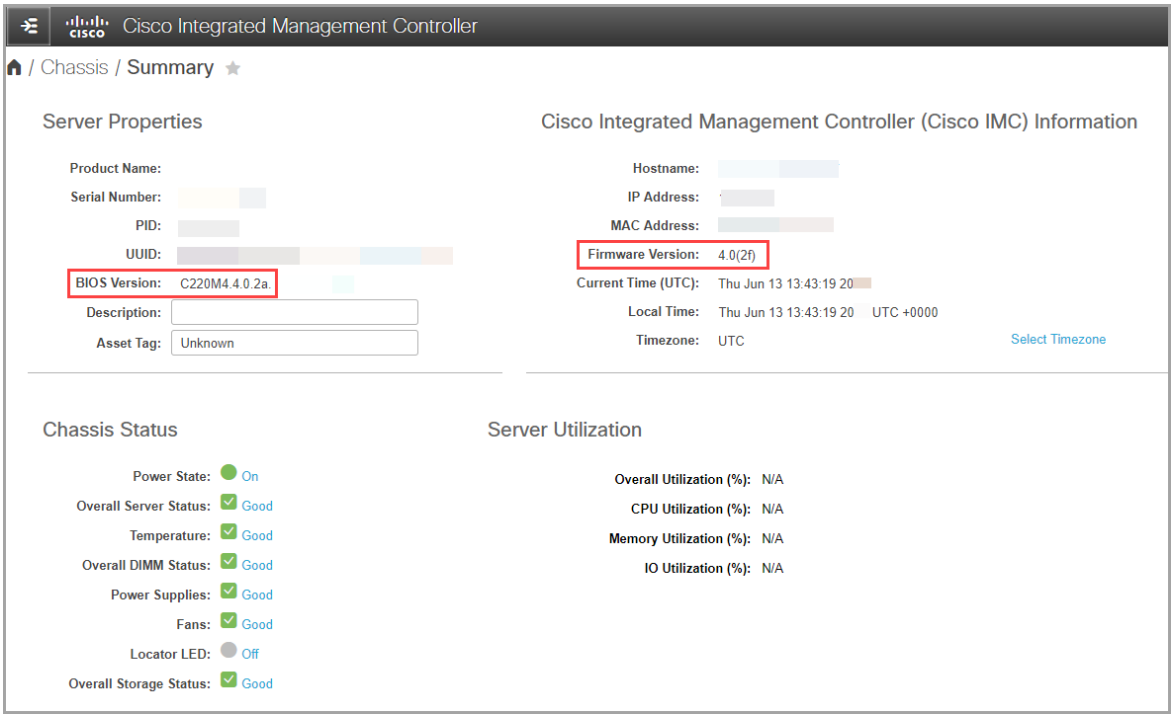
> 更新が成功したことを確認するには、「**更新の成功の確認**」を参照してください。

M5 ハードウェア（仮想コンソール）

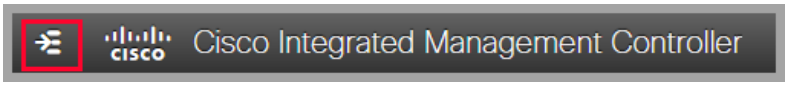
UCS M5 ハードウェアの CIMC および BIOS を更新するには、次の手順を実行します。

1. CIMC にログインします。
2. **BIOS バージョン**と**ファームウェアバージョン**をメモします。

   これらは、更新プログラムが正常にインストールされると変更されます。



3. ［ナビゲーションの切り替え（Toggle Navigation）］アイコンをクリックして、サイドメニューを表示します。

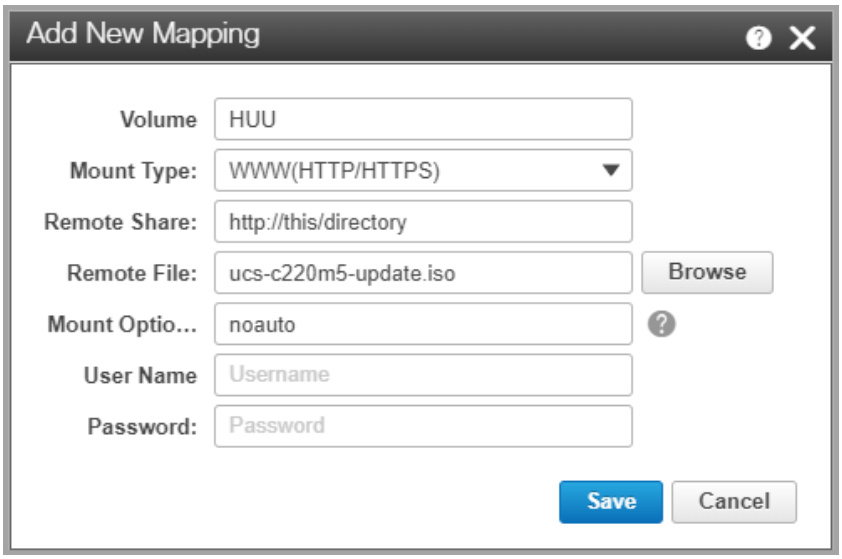


4. サイドメニューから［コンピューティング（Compute）］タブを選択します。
5. ［リモート管理（Remote Management）］タブ、［仮想メディア（Virtual Media）］タブの順に選択します。

> すでにマッピングされている別のファイルがある場合は、［マップ解除（Unmap）］と［削除（Delete）］をクリックしてそのファイルを削除し、新しい ISO ファイルをロードできるようにします。

6. ［新しいマッピングの追加（Add New Mapping）］をクリックします。

   ［新しいマッピングの追加（Add New Mapping）］ダイアログボックスが表示されます。



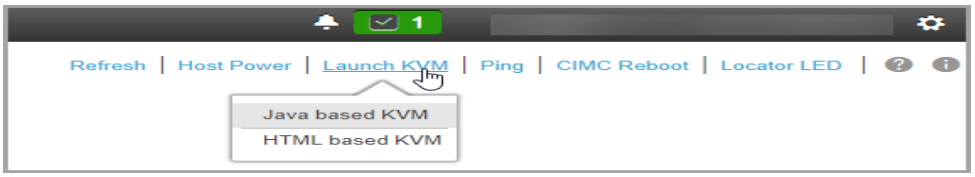
7. 次のフィールドに入力します。

   - [ボリューム(Volume)]フィールドに HUU と入力します。
   - [マウントタイプ(Mount Type)]フィールドで[WWW(HTTP/HTTPS)]を選択します。

   > 別のマウントタイプを選択する場合は、対応する通信ポートが有効になっていることを確認してください。

   - [リモート共有(Remote Share)]フィールドに ISO ファイルのファイル共有パスを入力します。
     例:**http://this/directory**
   - リモートファイルを選択します。
     例:**ucs-c220m5-update.iso**
   - [マウントオプション(Mount Options)]フィールドで[noauto]を選択します。
   - 要求された場合は、[ユーザ名(User Name)]と[パスワード(Password)]を入力します。

8. [保存(Save)]をクリックします。
9. [現在のマッピング(Current Mappings)]セクションを探し、[ステータス(Status)]列に[OK]と表示されていることを確認します。
10. [変更の保存(Save Changes)]をクリックします。
11. ツールバーから、[KVMの起動(Launch KVM)]を選択し、[JavaベースKVM(Java based KVM)]または[HTMLベースKVM(HTML based KVM)]を選択します。



[仮想コンソール(Virtual Console)]ダイアログボックスが表示されます。

12. [電源(Power)]を選択し、[システムのリセット(ウォーム ブート)(Reset System (Warm Boot))]を選択します。

    リブートプロセスが開始されます。

13. リブートプロセス中にブートメニューで F6 を選択します。

    [ブートデバイスを選択してください(Please Select Boot Device)]ダイアログボックスが表示されます。

14. [Cisco CIMC-Mapped vDVD1.22]を選択します。

    [シスコソフトウェアライセンス契約書(Cisco Software License Agreement)]ダイアログボックスが表示されます。

15. [同意します(I Agree)]をクリックします。

    [ファームウェアユーティリティの更新(Firmware Utility Update)]ダイアログボックスが表示されます。

16. [すべて更新&アクティブ化(Update & Activate All)]を選択します。
17. 画面に表示される指示に従って、更新を続行します。

    [ステータス(Status)]は[完了(Completed)]になるまで[進行中(In Progress)]と表示されます。これは時間がかかる場合があります。

    CIMC が更新され、再起動します。

> 更新が成功したことを確認するには、「**更新の成功の確認**」を参照してください。

USB デバイスでの ISO ファイルの使用

UCS アプライアンスに直接挿入されている USB デバイスから起動することで、CIMC と BIOS を更新します。

> ブート可能な USB デバイスを使用して更新するには、UCS アプライアンスに直接アクセスできる必要があります。

更新をインストールする前に、CIMC にログインして **BIOS バージョン**と**ファームウェアバージョン**を確認します。これらは、更新プログラムが正常にインストールされると変更されます。

更新する必要がある Stealthwatch アプライアンスを確認するには、「**StealthWatch アプライアンス**」を参照してください。すべての物理アプライアンスを必ず更新してください。

UCS M4 および M5 ハードウェア用の USB デバイスにマウントされた ISO を使用して CIMC および BIOS を更新する方法については、以下の **M4 および M5 ハードウェア**を参照してください。

ISO ファイル

ISO ファイルは、Cisco Stealthwatch Enterprise ダウンロードおよびライセンスセンターからダウンロードできます。

ブート可能な USB デバイス

ISO ファイルからブート可能な USB デバイスを作成する必要があります。ブート可能な USB デバイスを作成する方法は、プラットフォーム（Mac、PC、またはLinux）によって異なります。

M4 および M5 ハードウェア

USB デバイスに ISO をマウントして、UCS M4 および M5 ハードウェアの BIOS を更新するには、次の手順を実行します。

1. ブート可能な USB デバイスを UCS アプライアンスに挿入します。
2. Stealthwatch アプライアンスを再起動するか、電源をオンにします。
3. リブートプロセス中にブートメニューで F6 を選択します。

   [ブートデバイスを選択してください（Please Select Boot Device）] ダイアログボックスが表示されます。

4. USB デバイスを選択します。

   （これは USB ベンダーによって異なります）。

5. [シスコソフトウェアライセンス契約書（Cisco Software License Agreement）] ダイアログボックスが表示されたら、[同意します（I Agree）] をクリックします。

   [ファームウェアユーティリティの更新（Firmware Utility Update）] ダイアログボックスが表示されます。

6. [すべて更新&アクティブ化（Update & Activate All）] を選択します。
7. 画面に表示される指示に従って、更新を続行します。

   [ステータス（Status）] は [完了（Completed）] になるまで [進行中（In Progress）] と表示されます。これは時間がかかる場合があります。

   CIMC が更新され、再起動します。

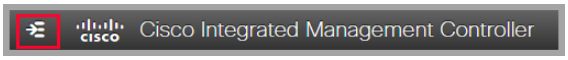
> 更新が成功したことを確認するには、「**更新の成功の確認**」を参照してください。

更新の成功の確認

次の手順に従って、更新が成功したことを確認します。

1. クレデンシャルを使用してログインします。

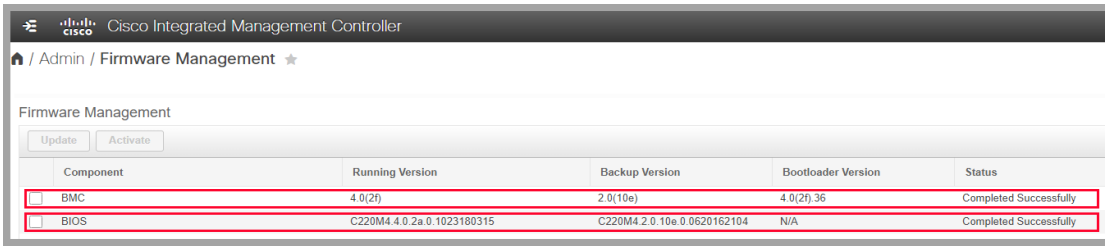
2. [ナビゲーションの切り替え(Toggle Navigation)]アイコンをクリックして、サイドメニューを表示します。



3. [管理(Admin)]を選択します。
4. [ファームウェア管理(Firmware Management)]を選択します。

   [管理/ファームウェア管理(Admin/Firmware Management)]ダイアログボックスが表示されます。

5. [実行中のバージョン(Running Version)]および[ステータス(Status)]列を確認して、CIMC(BMC)および BIOS がバージョン 4.0 に正常に更新されたことを確認します。



サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- Cisco Stealthwatch サポートのお問い合わせ先：
- Web でケースを開く場合：
  http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報