



## **Cisco IMC Supervisor リリース 2.1 ラックマウント サーバ管理 ガイド**

初版：2016年09月19日

最終更新：2017年03月06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/](http://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 ix

対象読者 ix

表記法 ix

マニュアルに関するフィードバック xi

マニュアルの入手方法およびテクニカル サポート xi

### このリリースの新規情報および変更情報 1

このリリースの新規情報および変更情報 1

### 概要 5

Cisco IMC Supervisor について 5

ライセンスについて 6

製品アクセス キーの契約履行 7

Cisco IMC Supervisor ユーザ インターフェイスの共通用語 8

ラック グループ 8

ラック アカウント 9

ポリシー 9

プロファイル 9

共通のユーザ インターフェイス オプション 9

Cisco IMC Supervisor ユーザ インターフェイスへのセキュアな接続の設定 11

Cisco IMC Supervisor ユーザ インターフェイスへの非セキュア接続の設定 12

### 使用する前に 15

概要 15

Cisco IMC Supervisor の起動 16

ライセンス タスク 17

ライセンスの更新 17

ライセンス監査の実行 18

ユーザ アクセス プロファイルの管理 18

マルチロール アクセス プロファイル	18
ユーザ アクセス プロファイルの作成	19
プロフィールへのログイン	20
Default Profile	20
デフォルト プロファイルの変更	21
認証および LDAP 統合	21
認証の環境設定	21
LDAP の設定	22
LDAP 統合	22
LDAP 統合の規則と制限事項	23
LDAP 設定の追加	25
LDAP サーバの設定	27
LDAP サーバのサマリー情報の表示	31
LDAP サーバの接続のテスト	31
ベース DN の検索	31
LDAP の手動同期のリクエスト	32
LDAP 同期の実行と LDAP 同期結果の表示	33
LDAP サーバの詳細の変更	33
グループ メンバーシップ情報の表示	35
LDAP サーバ情報の削除	35
SCP ユーザの設定	36
[Mail Setup] の設定	36
Cisco.com のユーザ クレデンシャルの設定とプロキシ設定	37
Cisco.com ユーザの設定	38
プロキシの設定	38
ブランド表示	39
新しいログインブランディング ページの追加	39
[User Interface Settings] の設定	40
ユーザとユーザ ロールの作成	43
概要	43
ユーザ アカウントの作成	45
オンライン ユーザの表示	46

ユーザ ロールの追加	46
ユーザ グループの追加	47
ユーザ グループのブランディング	48
グループ共有ポリシー	49
グループ共有ポリシーの追加	49
<b>サーバ検出、ラック グループ、およびラック アカウントの管理</b>	<b>51</b>
概要	51
サーバの検出およびインポート	52
自動検出プロファイルの設定	52
自動検出の実行	55
サーバのインポート	56
検出されたデバイスのプロパティの設定	57
ラック グループの追加	57
ラック アカウントの追加	58
ラック アカウントまたはラック グループのインベントリの収集	60
ラック グループへのラック アカウントの割り当て	61
アカウント接続のテスト	62
<b>インベントリ データおよび障害の表示</b>	<b>63</b>
ラックマウント サーバの詳細の表示	63
ラック マウント サーバの障害の詳細の表示	66
ラック グループのサマリー レポート	66
サーバ障害に関する電子メールアラート ルールの追加	67
<b>ラック サーバの管理</b>	<b>71</b>
ラックマウント サーバの詳細の表示	71
ラック マウント サーバの障害の詳細の表示	74
ラック マウント サーバの電源オン/オフ	75
ラックマウント サーバのシャットダウン	75
ラックマウント サーバのハードリセットの実行	76
ラック マウント サーバの電源再投入の実行	77
ラックマウント サーバの KVM コンソールの起動	77
ラックマウント サーバの GUI の起動	78
ラックマウント サーバのロケータ LED の設定	79

ラックマウント サーバのラベルの設定	80
ラックマウント サーバのタグの管理	80
ラックマウント サーバのタグの追加	84
リモート サーバへのテクニカル サポート データのエクスポート	85
SEL のクリア	87
システム タスクの管理	87
タスクの実行	88
<b>ポリシーとプロファイルの管理</b>	<b>91</b>
クレデンシャル ポリシー	91
クレデンシャル ポリシーの作成	92
ハードウェア ポリシー	92
ハードウェア ポリシーの作成	93
BIOS ポリシー	95
ディスク グループ ポリシー	96
FlexFlash ポリシー	97
IPMI Over LAN ポリシー	101
LDAP ポリシー	103
レガシー ブート順序ポリシー	104
ネットワーク構成ポリシー	105
ネットワーク セキュリティ ポリシー	109
NTP ポリシー	110
パスワードの有効期限ポリシー	111
高精度のブート順序ポリシー	112
RAID ポリシー	113
Serial over LAN ポリシー	115
SNMP ポリシー	116
SSH ポリシー	117
ユーザ ポリシー	118
仮想 KVM ポリシー	120
VIC アダプタ ポリシー	121
vMedia ポリシー	122
ゾーン分割ポリシー	123

既存の設定からのポリシーの作成	124
ハードウェア ポリシーの適用	126
ハードウェア ポリシーでの一般タスク	127
ハードウェア プロファイル	128
ハードウェア プロファイルの作成	129
既存の設定からのプロファイルの作成	129
ハードウェア プロファイルの適用	131
ハードウェア プロファイルでの一般タスク	132
タグ ライブラリ	133
タグ ライブラリの作成	133
ファームウェア プロファイル	135
ファームウェア管理メニュー	135
ローカル サーバへのイメージの追加	135
ローカル ファイル システムからのイメージのアップロード	137
ネットワーク サーバからのイメージの追加	137
ファームウェアのアップグレード	139
<b>Cisco IMC Supervisor の更新</b>	<b>141</b>
Cisco IMC Supervisor パッチの更新の概要	141
Cisco IMC Supervisor パッチ更新の確認	141
<b>スケジュールの管理</b>	<b>143</b>
スケジュール管理の概要	143
スケジュールの作成	143
<b>サーバ診断の実行</b>	<b>145</b>
サーバ診断の概要	145
サーバ設定ユーティリティ イメージの場所の設定	146
診断の実行	147
<b>Cisco IMC Supervisor 向け Smart Call Home</b>	<b>149</b>
Smart Call Home の概要	149
Smart Call Home の設定	149
障害コード	150
<b>Cisco UCS C3260 高密度ストレージ ラック サーバの管理</b>	<b>153</b>
Cisco UCS C3260 高密度ストレージ ラック サーバについて	153

Cisco UCS C3260 高密度ストレージラック サーバアーキテクチャの概要	154
Cisco UCS C3260の高密度ストレージラック サーバでCisco IMCスーパーバイザ ラック アカウントの追加	155
Cisco UCS C3260 ラック サーバの管理	156
シャーシ管理コントローラの再起動	156
Cisco UCS C3260 ラック サーバの前面ロケータ LED の設定	157
Cisco UCS C3260 ラック サーバのタグの管理	157
Cisco UCS C3260 ラック サーバのタグの追加	157
ポリシーとプロファイル	158
ファームウェアのアップグレード	160
Cisco UCS C3260 高密度ストレージラック サーバの詳細情報の表示	160
<b>サポート情報の表示</b>	<b>163</b>
サポート情報	163
サポート情報の表示	163
<b>頻繁に実行するタスクおよび手順</b>	<b>167</b>
頻繁に実行する手順	167
その他の手順	167
ダッシュボード ビューの有効化	168
ダッシュボードの自動更新の有効化	168
ダッシュボードへのサマリー レポートの追加	168
[Favorites] へのメニューまたはタブの追加	169
レポート テーブル ビューのカスタマイズ	169
レポートのフィルタリング	170
レポートのエクスポート	171





## はじめに

---

ここでは、次の項について説明します。

- [対象読者](#), [ix ページ](#)
- [表記法](#), [ix ページ](#)
- [マニュアルに関するフィードバック](#), [xi 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](#), [xi ページ](#)

## 対象読者

このマニュアルは、または を使用し、以下の少なくとも 1 つの分野において責任と専門知識を持つデータセンター管理者を主に対象としています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ
- 仮想化および仮想マシン

## 表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドラベルなどの GUI 要素は、イタリック体 ( <i>italic</i> ) で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルなどのメインタイトルは、ボールド体 ( <b>bold</b> ) で示しています。

テキストのタイプ	説明
マニュアルのタイトル	マニュアルのタイトルは、イタリック体 ( <i>italic</i> ) で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナルセッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体 ( <b>this font</b> ) で示しています。 CLI コマンド内の変数は、イタリック体 ( <i>italic</i> ) で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x y z}	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]	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。
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。
!、#	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。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



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。

**ヒント**

「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

**ワンポイントアドバイス**

「時間の節約に役立つ操作」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。装置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。

これらの注意事項を保管しておいてください。

## マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、毎月更新される『[What's New in Cisco Product Documentation](#)』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。





## 第 1 章

# このリリースの新規情報および変更情報

この章の内容は、次のとおりです。

- [このリリースの新規情報および変更情報, 1 ページ](#)

## このリリースの新規情報および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 1: *Cisco IMC Supervisor* リリース 2.1 の新機能と変更された動作

機能	説明	参照先
シャーシの管理	<p>Cisco UCS C3260 高密度ストレージラック サーバは、スタンドアロン環境で、Cisco IMC Supervisor と統合された Cisco Unified Computing System の一部として動作するように設計されています。</p> <p>Cisco IMC Supervisor で管理される高密度ストレージラックサーバは、Cisco IMC Supervisor を介して管理されるその他の C シリーズラックサーバによってサポートされる機能の一部をサポートします。</p>	<a href="#">Cisco UCS C3260 高密度ストレージラック サーバの管理, (153 ページ)</a>

機能	説明	参照先
RAID ポリシーの機能強化	RAID ポリシーの問題の修正のため、[Set disks in JBOD state to Unconfigured Good] チェックボックス、[Configure Unused Disks] チェックボックスなどの UI に変更が加えられています。	<a href="#">#unique_9</a>
ネットワーク構成ポリシーの導入	ネットワーク構成ポリシーを使用すると、DNS サーバおよびその他のネットワーク設定を設定できます。	<a href="#">#unique_10</a>
ユーザ ポリシーの機能強化	作成する強力なパスワードオプションをユーザに適用するために UI に変更が加えられています。	<a href="#">#unique_11</a>
ゾーン分割ポリシーの導入	ゾーン分割ポリシーを使用すると、サーバに物理ドライブを割り当てることができます。	<a href="#">ゾーン分割ポリシー</a> 、(123 ページ)
CSV からサーバをインポートする際にグループとタグを指定する機能の導入	自動検出プロファイルを設定する際、[IP Address CSV File] オプションを選択していると、CSV ファイルの一部のフィールドを指定できます。	<a href="#">自動検出プロファイルの設定</a> 、(52 ページ)
複数の KVM の選択と編集のサポート	KVM コンソールを起動するサーバは最大 5 台選択できます。	<a href="#">ラックマウントサーバの KVM コンソールの起動</a> 、(77 ページ)
SCU イメージの複数プロファイルのサポート	Cisco IMC Supervisor では、サーバが存在するさまざまな地理的場所にまたがる複数の診断イメージを設定できます。	<a href="#">サーバ診断の実行</a> 、(145 ページ)
ラックサーバ配下での高速化テスト接続の機能強化	1 つ以上のラック アカウントの接続テストを容易かつ迅速に行うことができます。	<a href="#">アカウント接続のテスト</a> 、(62 ページ)
電子メール ルールのカスタマイズの機能強化	電子メール ルールをカスタマイズして、個々のサーバを 1 つのグループに含めることができます。	<a href="#">サーバ障害に関する電子メールアラートルールの追加</a> 、(67 ページ)









## 第 2 章

### 概要

---

この章は、次の内容で構成されています。

- [Cisco IMC Supervisor について, 5 ページ](#)
- [ライセンスについて, 6 ページ](#)
- [製品アクセス キーの契約履行, 7 ページ](#)
- [Cisco IMC Supervisor ユーザ インターフェイスの共通用語, 8 ページ](#)
- [共通のユーザ インターフェイス オプション, 9 ページ](#)
- [Cisco IMC Supervisor ユーザ インターフェイスへのセキュアな接続の設定, 11 ページ](#)
- [Cisco IMC Supervisor ユーザ インターフェイスへの非セキュア接続の設定, 12 ページ](#)

## Cisco IMC Supervisor について

Cisco IMC Supervisor は、大規模なラックマウントサーバを管理できる管理システムです。ラックマウントサーバのグループを作成して、グループ単位でモニタリングや資産管理を行うことができます。

Cisco IMC Supervisor を使用して、次のタスクを実行できます。

- サーバの論理的なグループ化とグループごとのサマリーの表示
- 管理対象サーバのインベントリの収集
- サーバとグループのモニタリング
- ファームウェアのダウンロード、アップグレードおよびアクティベーションを含むファームウェアの管理
- サーバを検出、モニタ、管理し、ファームウェアアップグレードをプログラムで実行するためにノースバウンド REST API を提供します。

- 電源制御、LED 制御、ログの収集、KVM の起動、CIMC UI の起動など、スタンドアロンサーバのアクションの管理。
- ロールベース アクセス コントロール (RBAC) を使用したアクセスの制限
- 電子メール アラートの設定
- ポリシーおよびプロファイルを使用したサーバ プロパティの設定
- ファームウェアのアップデートまたはサーバ検出などのタスクを延期するためのスケジュールの定義
- UCS サーバ設定ユーティリティを使用したサーバのハードウェア問題の診断
- Cisco Smart Call Home による、プロアクティブな診断、アラート、修復案の提供
- Cisco UCS C3260 高密度ストレージラックサーバの管理
- ネットワーク構成ポリシーによる DNS サーバおよびその他のネットワーク設定の設定
- ゾーン分割ポリシーによるサーバへの物理ドライブの割り当て
- さまざまな地理的場所にまたがる複数の診断イメージの設定
- 個々のサーバを 1 つのグループに含めるための電子メール ルールのカスタマイズ

## ライセンスについて

Cisco IMC Supervisor では次の有効なライセンスが必要です。

- Cisco IMC Supervisor 基本ライセンス。
- Cisco IMC Supervisor 基本ライセンスのあとにインストールする Cisco IMC Supervisor バルクエンドポイントイネーブルメントライセンス。
- Cisco IMC Supervisor Advanced ライセンス。ポリシーやプロファイルの追加、編集、および削除は基本ライセンスで行えますが、サーバへのポリシーまたはプロファイルの適用には Advanced ライセンスが必要です。ポリシーを適用する際にこのライセンスがないとエラーが発生します。
- デフォルトの組み込み Cisco IMC Supervisor 評価ライセンス。評価ライセンスは、エンドユーザが Cisco IMC Supervisor をインストールし、すべてのサービスを初めて起動するときに自動的に生成されます。50 個のサーバに適用可能です。

**重要**

- Cisco IMC Supervisor の評価ライセンスを使用している場合は、このライセンスの有効期限（ライセンスが生成されてから 90 日）が切れると、インベントリおよびシステムヘルス情報（障害など）を取得できなくなることに注意してください。システムデータの更新だけでなく、新しいアカウントの追加もできなくなります。その時点で、Cisco IMC Supervisor のすべての機能を使用するには、永久ライセンスをインストールする必要があります。
- 評価時に追加したサーバの数が購入したサーバライセンスの数を超えると、インベントリ収集は評価時にすでに追加されているサーバの場合も行われますが、新しいサーバの追加は行えません。たとえば、評価時に約 100 台のサーバを追加し、購入しているのが 25 サーバライセンスの場合は、評価ライセンスの期限が切れた後に、新しいサーバを追加できなくなります。また、高度なライセンスなしでは設定に関連する操作を実行できなくなります。
- インポートされた数のサーバがライセンス使用制限を超えると、Cisco IMC Supervisor は、制限を超えない範囲内でのみサーバをインポートし、追加のサーバではエラー メッセージを表示します。

いずれのライセンスも、入手してインストールするためのプロセスは同じです。ライセンスを取得するには、次の手順を実行します。

- 1 Cisco IMC Supervisor をインストールする前に、Cisco IMC Supervisor ライセンス キーを生成し、証明書（製品アクセス キー）を要求します。
- 2 シスコのソフトウェア ライセンス サイトに製品アクセス キー（PAK）を登録します（[製品アクセス キーの契約履行](#)、[\(7 ページ\)](#) を参照してください）。
- 3 Cisco IMC Supervisor をインストールした後、[ライセンスの更新](#)、[\(17 ページ\)](#) の手順に従ってライセンスを更新します。
- 4 ライセンスが検証されると、Cisco IMC Supervisor の使用を開始できます。

実行可能な他のさまざまなライセンス タスクについては、「[ライセンス タスク](#)、[\(17 ページ\)](#)」を参照してください。

## 製品アクセス キーの契約履行

シスコのソフトウェア ライセンス サイトで製品アクセス キー（PAK）を登録するには、次の手順を実行します。

### はじめる前に

PAK 番号が必要です。

## 手順

- ステップ1 シスコ ソフトウェア ライセンスの [Web サイト](#) に移動します。
- ステップ2 [Product License Registration] ページに転送されたら、トレーニングを受けるか、[Continue to Product License Registration] をクリックして続行してください。
- ステップ3 [Product License Registration] ページで、[Get New Licenses from a PAK or Token] をクリックします。
- ステップ4 [Enter a Single PAK or TOKEN to Fulfill] フィールドに PAK 番号を入力します。
- ステップ5 [Fulfill Single PAK/TOKEN] をクリックします。
- ステップ6 PAK を登録するために、[License Information] でその他のフィールドに情報を入力します。

フィールド	説明
Organization Name	組織名。
Site Contact Name	サイトの連絡先の名前。
Street Address	組織の番地。
City/Town	市区町村名。
State/Province	都道府県名。
Zip/Postal Code	郵便番号。
Country	国名。

- ステップ7 [Issue Key] をクリックします。  
ライセンス契約した機能が表示され、デジタル ライセンス契約書と zip 圧縮のライセンス ファイルが電子メールに添付されて、ユーザ指定の電子メールアドレスに送信されます。

## Cisco IMC Supervisor ユーザインターフェイスの共通用語

### ラック グループ

ラック グループとは、物理ラックマウントサーバの論理グループです。ラック グループは、C シリーズまたは E シリーズ（またはその両方）サーバの単一のコンバージドインフラストラクチャ スタックを表します。必要に応じて、ラック グループを追加、変更、および削除することができます。



(注) 初めてログインすると、Cisco IMC Supervisor によって [Default Group] というタイトルのラックグループが提供されます。このラックグループにラックアカウントを追加したり、新しいラックグループを作成し、そのグループにラックアカウントを追加したりできます。ただし、このデフォルトのラックグループアカウントは削除できません。

## ラック アカウント

ラックアカウントは、Cisco IMC Supervisor に追加されるスタンドアロンラックマウントサーバです。複数のラックマウントサーバを Cisco IMC Supervisor に追加することができます。ラックマウントサーバを Cisco IMC Supervisor にアカウントとして追加すると、Cisco IMC Supervisor によってラックマウントサーバの設定が完全に可視化されます。また、Cisco IMC Supervisor を使用して、CシリーズおよびEシリーズラックマウントサーバをモニタおよび管理できます。ラックアカウントは、デフォルトグループまたは作成したグループへのラックグループに追加する必要があります。

## ポリシー

ポリシーは、Cisco IMC でのさまざまな属性設定を定義するための主要なメカニズムです。ポリシーは、複数のサーバにわたって設定の一貫性と反復可能性を確保するうえで役立ちます。包括的なポリシーセットを定義して使用すると、多数のサーバに類似する設定を適用できるので、一貫性、制御、予測可能性、自動化が促進されます。


## プロファイル

複数のポリシーを組み合わせ、ハードウェアプロファイルが形成されます。たとえば、1つのラックハードウェアプロファイル設定の詳細情報を複数のラックマウントサーバに適用することができます。いくつかの特定のラックマウントサーバにこのハードウェアプロファイルを関連付けることができます。これにより、複数のサーバにわたって設定の一貫性と反復可能性が確保されます。プロファイルを定義して使用すると、類似する設定が多数のサーバに適用されるため、一貫性、制御、予測可能性、自動化が促進されます。

## 共通のユーザインターフェイスオプション

次の表は、アプリケーションユーザインターフェイスのすべてのページで利用できるオプションについて説明します。これらのオプションは、すべてのページで同じタスクを実行します。

アイコン	ラベル	説明
	Refresh	ページ上の報告されたデータを更新します。
	Favorite	[Favorites] メニューにページを追加します。 このオプションを使用すると、頻繁にアクセスするページを簡単に表示できるようになります。
	Add	[Add] ダイアログ ボックスが表示されます。このダイアログ ボックスで新しいリソースを追加できます。
	Edit	[Edit] ダイアログ ボックスが表示されます。このダイアログ ボックスでリソースを編集できます。
	Customize Table	[Customize Report Table] ダイアログ ボックスが表示されます。このダイアログ ボックスで表示する列を選択できます。
	Export Report	[Export Report] ダイアログ ボックスが表示されます。このダイアログ ボックスでレポートをシステムにダウンロードできます。 次のいずれかの形式でレポートを生成できます。 <ul style="list-style-type: none"> <li>• PDF</li> <li>• CSV</li> <li>• XLS</li> </ul>
	Expand	ページに表示されているすべてのフォルダを展開します。
	Collapse	ページに表示されているすべてのフォルダを折りたたみます。

アイコン	ラベル	説明
	Add Advanced Filter	ページに追加のフィルタリングパラメータを提供します。
	Search Field	ページ上の特定のレコードをフィルタリングするためのキーワードを受け入れます。

## Cisco IMC Supervisor ユーザーインターフェイスへのセキュアな接続の設定

システムへのセキュアな接続を設定するには、次の手順を実行します。

### 手順

- ステップ 1** server.xml ファイルで、`redirectPort` パラメータの値を 443 に更新します。このファイルは、`/opt/infra/web_cloudmgr/apache-tomcat/conf/` ディレクトリにあります。

```
<Connector port="80" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="443"
maxHttpHeaderSize="65536"/>
```

- ステップ 2** web.xml ファイルの次の行をアンコメントします。

```
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

これらの行は、ファイル内の任意の場所に追加できます。

- ステップ 3** ユーザーインターフェイスを起動してシステムにログインします。

# Cisco IMC Supervisor ユーザ インターフェイスへの非セキュア接続の設定

デフォルトでは、Cisco IMC Supervisor ユーザ インターフェイスはセキュアモードで起動します。セキュアモードをバイパスし、非セキュアモード（HTTP）でユーザ インターフェイスを起動するには、次の手順を実行する必要があります。

## 手順

**ステップ 1** root としてログインします。

**ステップ 2** /opt/infra/web\_cloudmgr/apache-tomcat/conf/server.xml ファイルを次のように変更します。

a) 既存の 8080 ポート コネクタのタグをコメントアウトします。

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
redirectPort="443" maxHttpHeaderSize="65536"
URIEncoding = "UTF-8"/>
-->
```

b) 新しい 8080 ポート コネクタのタグとして次を追加します。

```
<Connector port="8080" protocol="HTTP/1.1"
maxThreads="150" minSpareThreads="4"
connectionTimeout="20000"
URIEncoding = "UTF-8" />
```

**ステップ 3** /opt/infra/web\_cloudmgr/apache-tomcat/webapps/app/WEB-INF/web.xml ファイルに <security-constraint> タグをコメントします。

```
<!--
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>*/</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
-->
```

**ステップ 4** サービスを再起動します。

**ステップ 5** ユーザ インターフェイスを起動してシステムにログインします。  
次の URL 形式を使用して非セキュアモードでシステムにログインできます。

http://<IP-Address>:8080 または http://<IP-Address>



セキュア モードと非セキュア モードの両方でユーザ インターフェイスを起動できます。

---





## 第 3 章

# 使用する前に

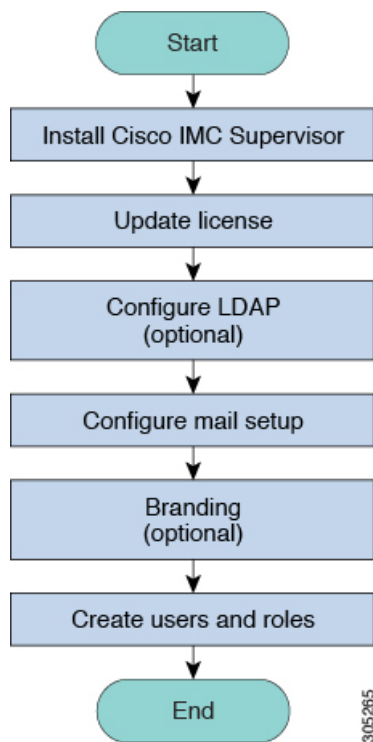
---

この章は、次の内容で構成されています。

- [概要, 15 ページ](#)
- [Cisco IMC Supervisor の起動, 16 ページ](#)
- [ライセンス タスク, 17 ページ](#)
- [ユーザ アクセス プロファイルの管理, 18 ページ](#)
- [認証および LDAP 統合, 21 ページ](#)
- [LDAP の設定, 22 ページ](#)
- [SCP ユーザの設定, 36 ページ](#)
- [\[Mail Setup\] の設定, 36 ページ](#)
- [Cisco.com のユーザ クレデンシャルの設定とプロキシ設定, 37 ページ](#)
- [ブランド表示, 39 ページ](#)
- [\[User Interface Settings\] の設定, 40 ページ](#)

## 概要

次の図は、Cisco IMC Supervisor を使用した環境設定のワークフローを示しています。



## Cisco IMC Supervisor の起動

Cisco IMC Supervisor は正常に正しく設定された IP アドレスで、インストールする必要があります。

### はじめる前に

- Cisco IMC Supervisor が正常にインストールされたことを確認します。
- Cisco IMC Supervisor のインストール中に IP アドレスを確実に設定します。

### 手順

ブラウザの URL に Cisco IMC Supervisor の IP アドレスを入力して、次のクレデンシャルでログインします。

- [User Name] : admin
- [Password] : admin

ログイン後、Cisco IMC Supervisor が起動します。Cisco IMC Supervisor のデフォルト ダッシュボードビューを表示します。

## ライセンス タスク

[License] メニューを使用して、ライセンスの詳細とリソースの使用率を確認できます。次のライセンス手順は、[Administration] > [License] メニューから使用できます。

タブ	説明
License Keys	このタブには、Cisco IMC Supervisor で使用されるライセンスの詳細が表示されます。このタブを使用してライセンスをアップグレードすることもできます。新しいバージョンの Cisco IMC Supervisor が使用可能な場合は、ライセンスをアップグレードできます。
License Utilization	このタブには、使用中のライセンスおよび各ライセンスの詳細（ライセンスの制限、使用可能期間、ステータス、備考など）が表示されます。ライセンスの監査もこのページから実行できます。
Resource Usage Data	このタブには、使用される各種リソースの詳細が表示されます。

## ライセンスの更新

Cisco IMC Supervisor の使用を始める前にライセンスを更新するには、次の手順を実行する必要があります。有効なライセンスのリストについては、[ライセンスについて](#)、(6 ページ) を参照してください。ライセンスキーを生成し、製品アクセスキーを要求し、登録する必要があります。Cisco IMC Supervisor をインストール後、ライセンスが検証され、Cisco IMC Supervisor の使用を開始できます。

### はじめる前に

ライセンス ファイルを圧縮ファイルで受け取った場合は、展開して .lic ファイルをローカル マシンに保存します。

### 手順

- 
- ステップ 1   メニュー バーで、[Administration] > [License] を選択します。
  - ステップ 2   [License Keys] タブを選択します。
  - ステップ 3   [Update License] をクリックします。
  - ステップ 4   [Update License] ダイアログボックスで、次のいずれかの操作を実行します。

- .lic ファイルをアップロードするには、[Browse] をクリックして .lic ファイルを探して選択し、[Upload] をクリックします。
- ライセンス キーの場合は、[Enter License Text] チェックボックスをオンにし、ライセンス キーのみをコピーして [License Text] フィールドに貼り付けます。ライセンス キーは通常、ファイルの先頭の Key -> の後にあります。  
ライセンス ファイルのフルテキストをコピーして [License Text] フィールドに貼り付けることもできます。

**ステップ 5** [Submit] をクリックします。  
ライセンス ファイルが処理されて、更新の成功を確認するメッセージが表示されます。

---

## ライセンス監査の実行

ライセンス監査を実行するには、次の手順を実行します。

### はじめる前に

ライセンスを更新する必要があります。ライセンスをアップグレードするには、[ライセンスの更新](#)、(17 ページ) を参照してください。

### 手順

---

- ステップ 1** メニュー バーで、[Administration] > [License] を選択します。
  - ステップ 2** [License Utilization] タブをクリックします。
  - ステップ 3** [Run License Audit] をクリックします。
  - ステップ 4** [Run License Audit] ダイアログボックスで、[Submit] をクリックします。  
このプロセスは完了するまでに時間がかかります。
  - ステップ 5** 確認ダイアログボックスで、[OK] をクリックします。
- 

## ユーザ アクセス プロファイルの管理

### マルチロール アクセス プロファイル

1 人のユーザを複数のロールに割り当てることができます。これは、1 つのユーザ アクセス プロファイルとしてシステム内で反映されます。たとえば、あるユーザが、グループ管理者、および全ポリシーの管理者として Cisco UCS Director にログインしようとした場合、両方のタイプのアクセスが適切であれば、いずれのログインも可能です。

アクセスプロファイルは、ユーザごとに表示できるリソースも定義します。Cisco UCS Director リリース 5.4 では、シングルユーザへの複数のプロファイルのサポートが導入されました。バージョン 5.4 をインストールし、ユーザアカウントが複数のグループに関連付けられている場合、システムはユーザアカウント用に複数のプロファイルを作成します。ただし、以前のバージョンからシステムをバージョン 5.4 にアップグレードし、[LDAPSyncTask] が実行されていない場合、デフォルトでは、1つのプロファイルだけが、システムのユーザアカウント用にリストされます。

LDAP ユーザを Cisco UCS Director に統合するときにユーザが複数のグループに属している場合、システムにより各グループのプロファイルが作成されます。ただし、デフォルトでは、ドメインユーザプロファイルが LDAP ユーザに追加されます。



(注) [Manage Profiles] 機能を使用して、ユーザアクセスプロファイルに対して追加、ログイン、編集、または削除を行うことができます。

## ユーザアクセス プロファイルの作成

### 手順

- ステップ 1 メニューバーで、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2 [Login User] タブを選択します。
- ステップ 3 リストからユーザを選択します。
- ステップ 4 [Manage Profiles] をクリックします。
- ステップ 5 [Manage Profiles] ウィンドウで、[add+] をクリックします。
- ステップ 6 [Add Entry to Access Profiles] ダイアログボックスで、次のフィールドに値を入力します。

フィールド名	説明
[Name] フィールド	プロファイル名。
[Description] フィールド	プロファイルの説明です。
[Type] ドロップダウン リスト	ユーザ ロールのタイプを選択します。
[Customer Organizations] ドロップダウン リスト	このユーザプロファイルを適用する組織を選択します。
[Show Resources From All Other Groups the User Has Access] チェックボックス	ユーザがアクセスできるか、属する他のグループすべてのリソースを表示できるようにするには、このチェックボックスをオンにします。

フィールド名	説明
[Shared Groups] フィールド	[Select] をクリックして、ユーザプロフィールを適用するグループを選択します。 ユーザは、選択されたグループに関連付けられたすべてのリソースにアクセスできます。
[Default Profile] チェックボックス	デフォルトのユーザアクセスプロフィールである場合は、このチェックボックスをオンにします。デフォルトでない場合は、このチェックボックスをオフにします。

**ステップ 7** [Submit] をクリックします。

#### 次の作業

必要に応じて、追加のユーザプロフィールを作成します。

## プロフィールへのログイン

システムのユーザとして、ユーザアカウントに対して複数のプロフィールがある場合、特定のプロフィールを使用してシステムにログインできます。

#### 手順

**ステップ 1** [Cisco UCS Director login] ダイアログボックスの [Username] フィールドに、ユーザ名を「ユーザ名: アクセスプロフィール名」の形式で入力します。

例: Alex: GrpAdmin

**ステップ 2** [Password] フィールドにパスワードを入力します。

**ステップ 3** [Login] をクリックします。

## Default Profile

デフォルトプロフィールは、システムで作成した最初のプロフィールです。デフォルトプロフィールを別のプロフィールに変更できます。新しいデフォルトプロフィールを使用し、ユーザ名とパスワードを入力してログインします。



## デフォルト プロファイルの変更

### 手順

- 
- ステップ 1** ユーザ インターフェイスで、右上隅に表示されているユーザ名をクリックします。ユーザ名は [logout] オプションの左側に表示されます。
- ステップ 2** [User Information] ウィンドウの [Access Profiles] タブを選択します。
- ステップ 3** ユーザ プロファイルを選択し、[Set as Default Profile] をクリックします。  
 (注) プロファイルは、追加または編集されている間、デフォルトとしても設定できません。
- 

## 認証および LDAP 統合

LDAP のフォールバックを選択して、認証を設定できます。また、フォールバックを行わない VeriSign ID 保護 (VID) 認証を設定できます。

名前	説明
[Local First, fallback to LDAP]	認証は最初にローカル サーバで実行されます (Cisco IMC Supervisor)。ユーザがローカル サーバにない場合、LDAP サーバが確認されます。
[VeriSign Identity Protection]	VIP 認証サービス (2 要素認証) が有効化されます。

## 認証の環境設定

ログイン認証タイプを変更する場合は、次の手順を実行します。

### 手順

- 
- ステップ 1** メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2** [Authentication Preferences] タブを選択します。
- ステップ 3** [Authentication Preferences] ドロップダウン リストから、次のオプションのいずれかを選択できます。
- [Local First, fallback to LDAP]

このオプションを選択する場合は、LDAP サーバを設定する必要があります。詳細については、[LDAP サーバの設定](#)、(27 ページ) を参照してください。

- [Verisign Identity Protection] : このオプションを選択した場合は、次のステップに進みます。

**ステップ 4** [Verisign Identity Protection] を選択した場合は、次の手順を実行します。

- a) VIP 証明書をアップロードするには、[Browse] をクリックします。  
証明書を見つけて選択し、[Upload] をクリックします。
- b) [Password] を入力します。

**ステップ 5** [Save] をクリックします。

---

## LDAP の設定

Cisco IMC Supervisor での LDAP の設定には、LDAP 設定の追加と LDAP サーバの設定が含まれます。また、LDAP の接続をテストし、LDAP の概要情報を表示できます。次の項では、これらの手順の実行方法について説明します。

## LDAP 統合

LDAP 統合を使用して、LDAP サーバのユーザを Cisco IMC Supervisor と同期できます。LDAP 認証により、同期されたユーザを LDAP サーバで認証することができます。LDAP ユーザを自動または手動で同期できます。LDAP アカウントの追加中に、LDAP アカウントが Cisco UCS Director と自動的に同期される頻度を指定できます。オプションで LDAPSynctask システム タスクを使用して、LDAP 同期を手動でトリガーすることもできます。

手動または自動で新しい組織単位 (OU) が LDAP ディレクトリに追加され、同期プロセスが実行されると、直近に追加された LDAP ユーザが Cisco IMC Supervisor に表示されます。

システム タスクを実行する機能に加えて、Cisco IMC Supervisor には LDAP ディレクトリとシステムを同期するための追加オプションもあります。

[Cleanup LDAP Users] システム タスク : このシステム タスクは、システム内で同期されたユーザが LDAP ディレクトリから削除されたかどうかを判別します。LDAP ディレクトリから削除されたユーザのレコードが存在する場合、このシステム タスクの実行後に、これらのユーザはシステム内で無効としてマークされます。管理者は、これらの非アクティブユーザのリソース割り当てを解除できます。デフォルトでは、このタスクは有効モードになっています。このシステム タスクが無効モードに設定されるのは、サービスを 2 回再起動した後だけです。

ローカルに存在している、または Cisco IMC Supervisor で外部から同期されているユーザは選択できません。

**重要**

グループ、またはドメイン ユーザのグループに属していないユーザは、[Users with No Group] として LDAP に表示されます。これらのユーザは、Cisco IMC Supervisor のドメイン ユーザのグループの下に追加されます。

異なる LDAP サーバアカウントに所属し、同じ名前を持った LDAP ユーザを追加できます。複数のユーザレコードを区別するために、ログインユーザ名の末尾にドメイン名が追加されます。たとえば、abc@vxdomain.com などです。このルールは、ユーザグループにも適用されます。

単一の LDAP アカウントが追加され、ユーザがユーザ名のみを指定してログインすると、Cisco IMC Supervisor は最初にそのユーザがローカルユーザまたは LDAP ユーザのどちらであるかを判別します。ユーザがローカルユーザおよび外部 LDAP ユーザの両方として識別された場合、ログイン段階でユーザ名がローカルユーザ名に一致すると、そのローカルユーザが Cisco IMC Supervisor に対して認証されます。あるいは、ユーザ名が外部ユーザの名前に一致すると、その LDAP ユーザが Cisco IMC Supervisor に対して認証されます。

## LDAP 統合の規則と制限事項

### グループの同期規則

- 選択した LDAP グループが Cisco IMC Supervisor にすでに存在しており、ソースのタイプが [Local] の場合、そのグループは同期中に無視されます。
- 選択した LDAP グループが Cisco IMC Supervisor にすでに存在しており、グループソースのタイプが [External] の場合、そのグループの説明および電子メール属性が Cisco IMC Supervisor で更新されます。
- LDAP サーバを追加する際には、ユーザフィルタとグループフィルタを指定できます。グループフィルタを指定すると、指定したグループに属するすべてのユーザがシステムに追加されます。さらに、次のような操作も行えます。
  - 指定したグループにサブグループが含まれている場合には、グループ、サブグループ、およびそれらのサブグループ内のユーザがシステムに追加されます（これが該当するのは、手動で LDAP ディレクトリを同期した場合のみです）。
  - ユーザが複数のグループの一部であり、グループフィルタとして指定されたグループに他のグループが一致しない場合、それらの追加グループはシステムに追加されません。
- ユーザは複数のユーザグループに属することができます。ただし、ユーザが属しているグループリストで最初に表示されているグループは、ユーザのデフォルトのプライマリグループとして設定されます。ユーザがどのグループにも属していない場合は、デフォルトのプライマリグループが [Domain Users] として設定されます。



(注) ユーザが属するすべてのグループに関する情報は、LDAPSyncTask システムタスクの実行後にのみ表示できます。

- LDAP グループを同期すると、グループ内のすべてのユーザが最初にシステムに追加されます。また、指定された LDAP グループ内のユーザが同じ OU 内の（または異なる OU 内の）他のグループに関連付けられている場合には、それらのグループも取得され、システムに追加されます。
- LDAP 同期プロセスでは、指定された LDAP グループが取得されてシステムに追加されると共に、ネストされたグループがあれば併せて追加されます。
- このリリースより前のリリースでは、ユーザは 1 つのグループにのみ属していました。ユーザが属するその他のグループは、最新リリースにアップグレードし、[LDAPSyncTask] システムタスクを実行した場合にのみ、[Manage Profiles] ダイアログボックスに表示されます。これは、他のグループが、LDAP サーバの設定時に指定したグループフィルタの条件に一致する場合のみ該当します。

#### ユーザの同期規則

- 名前に特殊文字が含まれている LDAP ユーザは Cisco IMC Supervisor に追加されます。
- LDAP サーバを追加する際には、ユーザフィルタとグループフィルタを指定できます。ユーザフィルタを指定すると、指定したフィルタに一致するすべてのユーザと、それらのユーザが属するグループが取得され、システムに追加されます。
- Cisco IMC Supervisor では、システムに追加された各ユーザのユーザプリンシパル名 (UPN) が表示されるようになりました。これは、以前のリリースでシステムに追加されたユーザに適用可能です。ユーザは、ログイン名またはユーザプリンシパル名を使用してシステムにログインできます。プロファイル名とともにユーザプリンシパル名を使用してのログインはサポートされていません。
- 選択した LDAP ユーザが Cisco IMC Supervisor にすでに存在しており、ソースのタイプが [Local] の場合、そのユーザは同期中に無視されます。
- 選択した LDAP ユーザが Cisco IMC Supervisor にすでに存在しており、ソースのタイプが [External] の場合、そのユーザの名前、説明、電子メール、および他の属性が更新されて使用できるようになります。
- ユーザアカウントが 2 つの異なる LDAP ディレクトリに作成されると、最初に同期された LDAP ディレクトリのユーザの詳細が表示されます。もう一方の LDAP ディレクトリからのユーザの詳細は表示されません。
- これらの LDAP ディレクトリが同期された後、LDAP 外部ユーザは、完全なドメイン名と共にユーザ名を指定して Cisco IMC Supervisor にログインする必要があります。たとえば、vxedomain.cisco.com\username など。ただし、Cisco IMC Supervisor に追加されている LDAP サーバディレクトリが 1 つしかない場合には、この規則は適用されません。

#### ユーザ同期の制限事項

- あるユーザが複数のグループメンバーシップを持っていても、そのユーザは Cisco IMC Supervisor では単一のグループメンバーシップを持つこととなります。



(注)

- Cisco IMC Supervisor 内のユーザとグループ（ローカルと LDAP の両方）の合計数を 10,000 以下に保つことをお勧めします。この数値を超えると、アプライアンスが遅くなったり応答しなくなることがあります。
- LDAP 同期プロセスの後に、ユーザが正しいグループに割り当てられていることを確認します。

### ベストプラクティス

何千もの LDAP オブジェクトを Cisco IMC Supervisor に同期させると、アプライアンスのパフォーマンスに問題が発生する可能性があります。必要な LDAP オブジェクトのみを同期するには、次の手順を実行します。

- 1 Cisco IMC Supervisor へのアクセス権が必要なすべてのユーザを含む LDAP グループを作成します。
- 2 それらのグループのみを Cisco IMC Supervisor に同期します。

## LDAP 設定の追加

LDAP 設定を追加するには、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Administration] > [LDAP Integration] を選択します。
- ステップ 2** LDAP 設定を追加するには [+] をクリックします。
- ステップ 3** [Add LDAP Configurations] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Account Name] フィールド	LDAP アカウント名。
[Server Type] ドロップダウン リスト	Microsoft Active Directory または Open LDAP を選択します。
[Server] フィールド	サーバのホスト名または IP アドレス。
[Enable SSL] チェックボックス	LDAP サーバへのセキュアな接続をイネーブルにします。

フィールド	説明
[Port] フィールド	ポート番号 SSL の場合は 636 に、非セキュアモードの場合は 389 に自動的に設定されます。
[Domain Name] フィールド	LDAP ユーザのドメイン名。
[Username] フィールド	LDAP ユーザの名前を入力します。
[Password] フィールド	ユーザ名に関連付けられているパスワードを入力します。
[Synchronization Frequency] ドロップダウンリスト	LDAP サーバが同期される頻度（時間）を選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• 1</li> <li>• 4</li> <li>• 12</li> <li>• 24</li> </ul>

**ステップ 4** [Next] をクリックします。

**ステップ 5** [LDAP Search Base] ダイアログボックスで [Select] をクリックして、表示されるテーブルから、OU に基づいてユーザを検索するための検索条件を選択します。

(注) Cisco IMC Supervisor ではユーザのみがサポートされ、グループはサポートされません。[OU] に基づく検索条件は必須ではありません（ユーザとグループの両方が含まれる可能性があるためです）。システム同期更新タスクが 24 時間ごとに実行され、検索基準に基づいて LDAP ユーザが同期更新されます。このため、ユーザ情報のみの手動同期を実行する必要があります。LDAP の手動同期を実行するには、[LDAP の手動同期のリクエスト](#)、(32 ページ) を参照してください。

**ステップ 6** [Select] ダイアログボックスで [Select] をクリックします。  
選択済みの検索条件が、[Search Base] フィールドの横に表示されます。

**ステップ 7** [LDAP Search Base] ダイアログボックスで [Next] をクリックします。

**ステップ 8** [LDAP User Role Filter] ダイアログボックスでユーザ ロール フィルタ テーブルにエントリを追加するには、[+] をクリックします。

**ステップ 9** [Add Entry to User Role Filters] ダイアログボックスで、ユーザ ロールの詳細を入力します。

**ステップ 10** [Submit] をクリックします。

**ステップ 11** [Submit Result] ダイアログボックスで、[OK] をクリックします。  
これらのフィルタを編集または削除することができます。また、上/下矢印を使ってフィルタを移動すると、優先順位を設定できます。

**ステップ 12** [LDAP User Role Filter] ダイアログボックスで、[Submit] をクリックします。

**ステップ 13** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## LDAP サーバの設定

Cisco IMC Supervisor では複数の LDAP サーバとアカウントを設定できます。LDAP アカウントを追加するときに、次の項目を指定できます。

- 検索ベース識別名 (DN) に含まれる組織単位 (OU)。
- LDAP アカウントがシステムと自動的に同期される頻度。
- 結果の数を制限し、グループおよびユーザに対する LDAP ロールフィルタを指定するグループフィルタまたはユーザフィルタ。

LDAP サーバアカウントが追加されると直ちにこのアカウントのシステムタスクが自動的に作成され、データ同期を即時に開始します。LDAP サーバアカウントのすべてのユーザとグループがシステムに追加されます。デフォルトでは、LDAP アカウントのすべてのユーザに対して、自動的にサービスエンドユーザプロファイルが割り当てられます。

### はじめる前に

認証設定を [Local First, fallback to LDAP] に設定しておく必要があります。

### 手順

**ステップ 1** メニューバーで、[Administration] > [LDAP Integration] を選択します。

**ステップ 2** [Add] をクリックします。

**ステップ 3** [LDAP Server Configuration] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Account Name] フィールド	アカウント名。 この名前は一意である必要があります。
[Server Type] フィールド	LDAP サーバのタイプ。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• OpenLDAP</li> <li>• MSAD - Microsoft Active Directory</li> </ul>
[Server] フィールド	LDAP サーバの IP アドレスまたはホスト名。

名前	説明
[Enable SSL] チェックボックス	LDAP サーバへのセキュアな接続をイネーブルにします。
[Port] フィールド	ポート番号 SSL の場合は 636 に、非セキュアモードの場合は 389 に自動的に設定されます。
[Domain Name] フィールド	ドメイン名。 LDAP ディレクトリのタイプとして [OpenLDAP] を選択した場合は、このドメイン名が、ユーザ名で指定されたドメインと一致している必要があります。 <b>重要</b> 完全なドメイン名を指定する必要があります。たとえば、vxedomain.com などです。
[Username] フィールド	ユーザ名。 LDAP ディレクトリのタイプとして [OpenLDAP] を選択した場合は、ユーザ名を次の形式で指定してください。 <code>uid=users,ou=People,dc=ucsd,dc=com</code> ここに指定する <code>ou</code> は、ディレクトリ階層でその他のすべてのユーザが配置される場所です。
[Password] フィールド	ユーザのパスワード。
[Synchronization Frequency] ドロップダウンリスト	LDAP サーバが同期される頻度（時間）を選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• 1</li> <li>• 4</li> <li>• 12</li> <li>• 24</li> </ul>

**ステップ 4** [Next] をクリックします。

**ステップ 5** [LDAP Search Base] ペインで、[Select] をクリックして LDAP 検索ベースのエントリを指定し、[Select] をクリックします。

Cisco IMC Supervisor で使用可能なすべての組織単位（OU）がこのリストに表示されます。



**ステップ 6** [Next] をクリックします。

**ステップ 7** [Configure User and Group Filters] ペインで、次のフィールドに入力します。

名前	説明
[User Filters]	[+] 記号をクリックして、システムと同期する必要がある特定のユーザを選択します。 選択したユーザが属するグループがすべて取得され、システムに追加されます。
[Group Filters]	[+] 記号をクリックして、システムと同期する必要があるグループを選択します。 選択したグループに属するユーザがすべて取得されて、システムに追加されます。ただし、選択したグループのユーザが選択していないその他のグループにも属している場合、それらのグループは、このフィールドで選択されている場合を除き取得されません。
[Add Entry to User Filters] または [Add Entry to Group Filters] ダイアログボックス（前の選択に応じて表示されます）	
[Attribute Name] ドロップダウン リスト	[Group Name] または [User Name] を選択します。
[Operator] ドロップダウン リスト	グループおよびユーザを取得する際に適用するフィルタを選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• [Equals to]</li> <li>• [Starts with]</li> </ul>
[Attribute Value] フィールド	検索に含めるキーワードまたは値を指定します。

フィルタに基づいて、グループまたはユーザが取得されます。

**ステップ 8** [Next] をクリックします。

**ステップ 9** [LDAP User Role Filter] ペインで、[+] 記号をクリックして、ユーザロールフィルタを追加します。

**ステップ 10** [Add Entry to User Role Filters] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Attribute Name] フィールド	属性の名前。これには、グループ名を指定できます。

名前	説明
[Operator] ドロップダウン リスト	ドロップダウンリストは次のいずれかになります。 <ul style="list-style-type: none"> <li>• [Equal to]</li> <li>• [Starts with]</li> </ul>
[Attribute Value] フィールド	このフィールドで値を指定します [Operator] フィールドと [Attribute Value] フィールドの値に一致するすべてのユーザが、[Map User Role] ドロップダウンリストで選択するユーザ ロールに割り当てられます。
[Map User Role] ドロップダウンリスト	ユーザのマップ先とするユーザ ロールを選択します。デフォルトで使用可能だったロールを選択するか、またはシステムで作成されたロールを選択できます。 以下は、Cisco IMC Supervisor でデフォルトで使用可能なロールです。 <ul style="list-style-type: none"> <li>• グループ管理者</li> <li>• オペレーター</li> <li>• システム管理者</li> </ul>

**ステップ 11** [Submit] をクリックします。

**ステップ 12** [OK] をクリックします。

ユーザ ロール フィルタが [User Role Filters] テーブルに追加されます。

(注) 複数のユーザ ロール フィルタが指定されている場合は、最初の行に指定したフィルタが処理されます。

ユーザのロールを手動で更新すると、そのユーザには、グループをマップしたユーザ ロールが適用されなくなります。

### 次の作業

LDAP に認証設定を設定していない場合は、認証設定を変更するように求めるプロンプトが表示されます。認証設定の変更の詳細については、[認証の環境設定](#)、(21 ページ) を参照してください。

## LDAP サーバのサマリー情報の表示

LDAP サーバの概要情報を表示するには、次の手順を実行します。

### 手順

- 
- ステップ 1 メニューバーで、[Administration] > [LDAP Integration] を選択します。
  - ステップ 2 表から LDAP アカウント名を選択します。
  - ステップ 3 [View] をクリックします。  
[View LDAP Account Information] 画面には、LDAP アカウントの概要情報が表示されます。
  - ステップ 4 [Close] をクリックします。
- 

## LDAP サーバの接続のテスト

LDAP 接続をテストするには、次の手順を実行します。

### 手順

- 
- ステップ 1 メニューバーで、[Administration] > [LDAP Integration] を選択します。
  - ステップ 2 テーブルから LDAP のアカウント名を選択します。
  - ステップ 3 [Test Connection] をクリックします。  
接続のステータスが表示されます。
  - ステップ 4 [Test LDAP Connectivity] ダイアログボックスで、[Close] をクリックします。
- 

## ベース DN の検索

ベース DN を検索するには、次の手順を実行します。

### 手順

- 
- ステップ 1 メニューバーで、[Administration] > [LDAP Integration] を選択します。
  - ステップ 2 [Search BaseDN] をクリックします。  
(注) Cisco IMC Supervisor ではユーザのみがサポートされ、グループはサポートされません。  
[OU] に基づく検索条件は必須ではありません (ユーザとグループの両方が含まれる可能性があるためです)。

- ステップ3 [LDAP Search Base] ダイアログボックスの [Select] をクリックします。
- ステップ4 1人以上のユーザを選択して、[Select] ダイアログボックスの [Select] をクリックします。
- ステップ5 [LDAP Search Base] ダイアログボックスの [Submit] をクリックします。
- ステップ6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

## LDAPの手動同期のリクエスト

LDAPの手動同期のリクエストでは、LDAP ユーザおよびグループを取得するための基本検索条件または詳細検索条件を指定できます。LDAPの手動同期を行うには、次の手順を実行します。

### 手順

- ステップ1 メニューバーで、[Administration] > [LDAP Integration] を選択します。
- ステップ2 [Request Manual LDAP Sync] をクリックします。
- ステップ3 [Manual LDAP Sync] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Basic Search] チェックボックス	組織単位で基本検索をイネーブルにします。
[Advanced Search] チェックボックス	詳細検索をイネーブルにします。

(注) いずれかの検索オプションを使用する時点ですでにユーザおよびグループが Cisco IMC Supervisor に存在している場合、検索を実行しても同じユーザとグループは読み込まれません。

- ステップ4 基本検索の場合は、[Select] をクリックして検索ベースを指定します。
- ステップ5 検索ベース DN を選択し、[Select] をクリックして、ステップ9に進みます。
- ステップ6 詳細検索の場合は、[Advanced Filtering Options] ペインで、[User Filters] と [Group Filters] の属性名を追加または編集します。
- ステップ7 [Next] をクリックします。
- ステップ8 [Select Users and Groups] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[LDAP Groups] フィールド	ユーザが同期する必要がある LDAP グループ。
[LDAP Users] フィールド	同期する必要がある LDAP ユーザ。

- ステップ9 [Submit] をクリックします。
- ステップ10 [Submit Result] ダイアログボックスで、[OK] をクリックし、LDAP サーバを同期します。

メニューバーから [Administration] > [Users and Groups] を選択し、[Users] タブをクリックすると、同期されたユーザが表示されます。

## LDAP 同期の実行と LDAP 同期結果の表示

LDAP の同期を実行し、結果を表示するには、次の手順を実行します。

### 手順

- ステップ 1 [Administration] > [System] を選択します。
- ステップ 2 [System] ページで、[System Tasks] をクリックします。
- ステップ 3 [User and Group Tasks] を展開し、[LDAPSyncTask] を選択します。
- ステップ 4 [Run Now] をクリックします。
- ステップ 5 [Submit] をクリックします。
- ステップ 6 (任意) [Manage Task] をクリックして、同期プロセスを有効または無効にします。

### 次の作業

同期プロセスの結果が Cisco IMC Supervisor に表示されます。[LDAP Integration] ページで、LDAP アカウントを選択し、[Results] をクリックして同期プロセスの概要を表示します。

## LDAP サーバの詳細の変更

設定済みの LDAP サーバに対し変更できるのは次の詳細情報のみです。

- ポート番号と SSL 設定
- ユーザ名とパスワード
- 同期頻度
- 検索ベース DN の選択内容
- マッピングされたユーザ ロールとグループ

LDAP サーバの詳細を変更するには、次の手順を実行します。

## 手順

- ステップ 1 [Administration] > [LDAP Integration] を選択します。
- ステップ 2 LDAP アカウントを選択します。
- ステップ 3 [Modify] をクリックします。
- ステップ 4 [LDAP Server Configuration] 画面で、次のフィールドを編集します。

名前	説明
[Enable SSL] チェックボックス	LDAP サーバへのセキュアな接続をイネーブルにします。
[Port] フィールド	ポート番号 SSL の場合は 636 に、非セキュアモードの場合は 389 に自動的に設定されます。
[Username] フィールド	ユーザ名。 LDAP ディレクトリのタイプとして [OpenLDAP] を選択した場合は、ユーザ名を次の形式で指定してください。 <code>uid=users,ou=People,dc=ucsd,dc=com</code> ここに指定する <code>ou</code> は、ディレクトリ階層でその他のすべてのユーザが配置される場所です。
[Password] フィールド	ユーザのパスワード。
[Synchronization Frequency] ドロップダウンリスト	LDAP サーバがシステムデータベースと同期される頻度（時間単位）を選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"><li>• 1</li><li>• 4</li><li>• 12</li><li>• 24</li></ul>

- ステップ 5 [Next] をクリックします。
- ステップ 6 [LDAP Search Base] エントリを編集し、[Next] をクリックします。
- ステップ 7 [User Filters] および [Group Filters] テーブルで必要な属性を選択して編集し、[Next] をクリックします。
- ステップ 8 [LDAP User Role Filter] テーブルでエントリを選択して編集します。
- ステップ 9 上矢印と下矢印を使用して、テーブルエントリの追加、編集、削除、または移動をクリックします。
- ステップ 10 [Submit] をクリックします。

## グループメンバーシップ情報の表示

システム内のユーザは、複数のユーザグループに属することができます。ユーザがシステムに追加されると、ユーザが属するすべてのグループもシステムに追加されます。ただし、最後にユーザが追加されたグループは、そのユーザのデフォルトのプライマリグループとして設定されます。ユーザがどのグループにも属していない場合は、デフォルトのプライマリグループが [Domain Users] として設定されます。[Manage Profiles] オプションを使用して、ユーザのグループメンバーシップを表示し変更することができますが、Cisco UCS Director では特定のユーザが属しているすべてのグループのリストを表示する追加オプションもあります。

### 手順

- ステップ 1 メニューバーで、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2 [Users] をクリックします。
- ステップ 3 テーブルからユーザを選択します。
- ステップ 4 [Group Membership] をクリックします。  
[Member Of] 画面に、ユーザが属するすべてのグループが表示されます。
- ステップ 5 [Close] をクリックします。

## LDAP サーバ情報の削除

LDAP サーバのアカウントを削除すると、検索基準、BaseDN および対象の LDAP サーバに関するシステム エントリのみが削除されます。LDAP サーバに割り当てられているユーザは削除されません。LDAP サーバ情報を削除するには、次の手順を実行します。

## 手順

- 
- ステップ 1 メニューバーから、[Administration] > [Users and Groups] の順に選択します。
  - ステップ 2 [LDAP Integration] タブを選択します。
  - ステップ 3 テーブルから LDAP のアカウント名を選択します。
  - ステップ 4 [Delete] をクリックします。
  - ステップ 5 確認のダイアログボックスで [Delete] をクリックします。
  - ステップ 6 [OK] をクリックします。
- これにより、Cisco IMC Supervisor 内の LDAP アカウントの削除が開始されます。LDAP アカウント内のユーザ数によって、この削除プロセスが完了するまでに数分かかる場合があります。この間、LDAP アカウントが Cisco IMC Supervisor に表示され続ける場合があります。[Refresh] をクリックして、アカウントが削除されたことを確認します。
- 

# SCP ユーザの設定

SCP ユーザは、サーバ診断やテクニカルサポートのアップロード操作で、SCP プロトコルを使用して Cisco IMC Supervisor アプライアンスにファイルを転送する際に使用されます。scp ユーザアカウントは、Cisco IMC Supervisor UI または shelladmin へのログインに使用することはできません。scp ユーザパスワードを設定するには、次の手順を実行します。

## 手順

- 
- ステップ 1 メニューバーから、[Administration] > [Users and Groups] の順に選択します。
  - ステップ 2 [SCP User Configuration] タブをクリックします。
  - ステップ 3 [Password] フィールドに scp ユーザパスワードを入力します。
  - ステップ 4 [Submit] をクリックします。
  - ステップ 5 [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

# [Mail Setup] の設定

Cisco IMC Supervisor から送信されるすべての電子メールに SMTP サーバが必要です。障害のアラートなどの Cisco IMC Supervisor によって生成される電子メールは、次の手順を使用して設定した電子メール設定に送信されます。電子メールアラートのルールを追加する方法の詳細については、[サーバ障害に関する電子メールアラートルールの追加](#)、(67 ページ) を参照してください。



## 手順

- ステップ 1** メニューバーで、[Administration] > [System] を選択します。
- ステップ 2** [Mail Setup] タブをクリックします。
- ステップ 3** [Mail Setup] ペインで、次のフィールドに値を入力します。

フィールド	説明
[Outgoing Email Server (SMTP)]	サーバの IP アドレスまたはドメイン名。
[Outgoing SMTP Port]	SMTP サーバのポート番号。
[Outgoing SMTP User]	(オプション) SMTP 認証で使用する送信 SMTP ユーザ ID。
[Outgoing SMTP Password]	(オプション) SMTP 認証で使用する送信 SMTP ユーザ ID のパスワード。
[Outgoing Email Sender Email Address]	Cisco IMC Supervisor によって生成される送信電子メールの送信者アドレス。
[Server IP Address]	Cisco IMC Supervisor を実行しているサーバの IP アドレス。
[Send Test Email] チェックボックス	設定されたアドレスにテストメールを送信するには、このチェックボックスをオンにします。

- ステップ 4** [Save] をクリックします。
- ステップ 5** 確認ダイアログボックスで、[OK] をクリックします。

## Cisco.com のユーザクレデンシャルの設定とプロキシ設定

シスコユーザクレデンシャルとプロキシの詳細は、[Administration] > [System] から設定できます。Cisco.com のユーザクレデンシャルとプロキシクレデンシャルは、アプリケーション全体の設定です。これらのクレデンシャルは、ファームウェアイメージのダウンロードと Cisco IMC Supervisor の更新に自動的に使用されます。Cisco Smart Call Home でも、これらのプロキシの詳細を使用します。

## Cisco.com ユーザの設定

Cisco.com のユーザ名とパスワードを設定する場合は、次の手順を実行します。

### 手順

- ステップ 1 [Administration] > [System] を選択します。
- ステップ 2 [System] ページで、[Cisco.com User Configuration] をクリックします。
- ステップ 3 次の項目を入力して、Cisco.com のユーザを設定します。

フィールド	説明
[User Name (cisco.com)] フィールド	シスコのログイン ユーザ名を入力します。
[Password (cisco.com)] フィールド	シスコのログイン パスワードを入力します。

- ステップ 4 [Save] をクリックします。

## プロキシの設定

プロキシ設定を構成する場合は、次の手順を実行します。

### 手順

- ステップ 1 [Administration] > [System] を選択します。
- ステップ 2 [System] ページで、[Proxy Configuration] をクリックします。
- ステップ 3 次の項目を入力してプロキシを設定します。

フィールド	説明
[Enable Proxy Configuration] チェックボックス	<p>(任意) このチェックボックスをオンにしてプロキシを有効化し、次の情報を入力します。</p> <ul style="list-style-type: none"> <li>• [Host Name] フィールド: プロキシ設定用のホスト名を入力します。</li> <li>• [Port] フィールド: プロキシ設定用のポートを入力します。</li> </ul>

フィールド	説明
[Enable Proxy Authentication] チェックボックス	<p>(任意) このチェックボックスをオンにしてプロキシ認証を有効化し、次の情報を入力します。</p> <ul style="list-style-type: none"> <li>• [Proxy User Name] フィールド: プロキシ認証用のプロキシユーザ名を入力します。</li> <li>• [Proxy Password] フィールド: プロキシユーザ名のパスワードを入力します。</li> </ul>

**ステップ 4** [Save] をクリックします。

## ブランド表示

ログイン ページは、ドメイン名に関連付けられているロゴを示すように設定できます。エンドユーザがそのドメインからログインすると、ログイン ページでそのカスタム ロゴが表示されます。ロゴの最適なイメージのサイズは幅 890 ピクセル、高さ 470 ピクセルで、余白に 255 ピクセルが割り当てられています。シスコは、より高速なダウンロードを実現するために、イメージサイズを小さくすることを推奨しています。

## 新しいログイン ブランディング ページの追加

新しいログイン ブランディング ページを追加する場合は、次の手順を実行します。

### 手順

- ステップ 1** メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2** [Login Page Branding] タブをクリックします。
- ステップ 3** [Add] をクリックします。
- ステップ 4** [Domain Branding] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Domain Name] フィールド	ブランディング用のドメイン名。たとえば、 <code>imcs.xxxx.com</code> のようになります。 (注) ローカルマシンでドメイン名を作成するには、 C:\Windows\System32\drivers\etcに移動して、ホストファイルで <ipaddress> と <domainname> を指定します。たとえば、 <code>10.10.10.10 imcs.xxxx.com</code> のようになります。
[Custom Domain Logo] チェックボックス	(オプション) ログを追加する場合は、このチェックボックスをオンにして、以下を実行します。  <ol style="list-style-type: none"> <li>1 [Browse] をクリックします。</li> <li>2 ログに移動してファイルを選択します。</li> <li>3 [Open] をクリックします。</li> </ol>

ステップ 5 [Submit] をクリックします。

ステップ 6 確認ダイアログボックスで、[OK] をクリックします。  
(注) 作成したカスタマイズ済みのログインページを編集、削除、複製できません。

## [User Interface Settings] の設定

この手順を使用して、Cisco IMC Supervisor アプリケーションをカスタマイズすることができます。要件に基づいて、アプリケーションヘッダー、管理者およびエンドユーザのポータルを変更できます。ロゴ、アプリケーション名、ログアウトなどのリンクを含むヘッダーも非表示にできます。

### 手順

ステップ 1 メニューバーで、[Administration] > [User Interface Settings] を選択します。

ステップ 2 [User Interface Settings] ウィンドウで、次の手順を実行します。

フィールド	説明
[Hide Entire Header] チェックボックス	このチェックボックスを使用して、ヘッダーを有効または無効にします。
[Product Name] フィールド	ヘッダーのメインタイトル。

フィールド	説明
[Product Name 2nd Line] フィールド	ヘッダーのサブタイトル。
[Enable About Dialog] チェックボックス	このチェックボックスを使用して、Cisco IMC Supervisor の [About] ダイアログボックスを有効または無効にします。
<b>管理者ポータル</b>	
[Custom Link 1 Label] フィールド	ヘッダーバーのテキストを変更するには、このフィールドを設定します。
[Custom Link 1 URL] フィールド	カスタム リンク 1 ラベルの URL を設定できます。
[Custom Link 2 Label] フィールド	ヘッダーバーのテキストを変更するには、このフィールドを設定します。
[Custom Link 2 URL] フィールド	カスタム リンク 2 ラベルの URL を設定できます。
<b>エンド ユーザ ポータル</b>	
[Custom Link 1 Label] フィールド	ヘッダーバーのテキストを変更するには、このフィールドを設定します。
[Custom Link 1 URL] フィールド	カスタム リンク 1 ラベルの URL を設定できます。
[Custom Link 2 Label] フィールド	ヘッダーバーのテキストを変更するには、このフィールドを設定します。
[Custom Link 2 URL] フィールド	カスタム リンク 2 ラベルの URL を設定できます。

**ステップ 3** [Save] をクリックします。

**ステップ 4** 確認ダイアログボックスで、[OK] をクリックします。





## 第 4 章

# ユーザとユーザ ロールの作成

この章は、次の内容で構成されています。

- [概要, 43 ページ](#)
- [ユーザ アカウントの作成, 45 ページ](#)
- [オンライン ユーザの表示, 46 ページ](#)
- [ユーザ ロールの追加, 46 ページ](#)
- [ユーザ グループの追加, 47 ページ](#)
- [ユーザ グループのブランディング, 48 ページ](#)
- [グループ共有ポリシー, 49 ページ](#)

## 概要

Cisco IMC Supervisor は、次のシステム定義のユーザ ロールをデフォルトでサポートしています。

- **[System Admin]** : ユーザの追加を含むすべての権限を持つユーザ。Cisco IMC Supervisor では、管理者として、システムによって提供されたユーザ ロールもしくはカスタム定義されたユーザ ロールを、ユーザに割り当てることができます。後で、割り当て済みのロールの情報を確認することもできます。次の割り当てを行うことができます。

- システムのカスタム ユーザ ロールを作成し、このロールを持つ新しいユーザ アカウントを作成するか、既存のユーザにロールを割り当てます。

新しいユーザ ロールの作成時に、そのロールを管理者またはオペレータのロールにするかを指定できます。ユーザ アカウントの作成の詳細については、[ユーザ アカウントの作成, \(45 ページ\)](#) を参照してください。ユーザ ロールの作成の詳細については、[ユーザ ロールの追加, \(46 ページ\)](#) を参照してください。

- 既存のユーザ ロール (デフォルトのロールを含む) を変更し、そのロールに関連付けられているユーザのメニュー設定と読み取り/書き込み権限を変更する。

ロールのメニュー設定と権限の変更手順は、ユーザ ロールの作成時の手順と同じです。

- **[Group Admin]** : すべての権限を持つユーザ。システム定義のユーザ グループ **[Default Group]** は、Cisco IMC Supervisor ではデフォルトで使用できます。グループ管理者として、ユーザ アカウントを作成してこのグループに割り当てたり、作成済みのグループにユーザ アカウントを割り当てたりできます。ユーザは複数のユーザ グループに属することができます。ただし、最後にユーザが追加されたグループは、そのユーザのデフォルトのプライマリ グループとして設定されます。
- **[Operator]** : システム管理者のロールタイプは **admin** であるため、アクセス制限（メニュー設定とユーザ権限）の任意の組み合わせを使用して、既存の **Operator** ロールを必要に応じて変更できます。デフォルトでは、以下のメニュー設定とユーザ権限が **Operator** に割り当てられます。

メニュー設定	ユーザ権限
システム : <ul style="list-style-type: none"> <li>• インベントリと障害のステータス</li> <li>• 物理アカウント</li> <li>• ファームウェア管理</li> <li>• サーバ診断</li> </ul>	<ul style="list-style-type: none"> <li>• 読み取り : 物理コンピューティング</li> <li>• 書き込み : 物理コンピューティング</li> <li>• 読み取り : システム管理者</li> <li>• 読み取り : ユーザ</li> <li>• 読み取り : タグ ライブラリの読み取り</li> <li>• 書き込み : タグ ライブラリの書き込み</li> <li>• 読み取り : オーケストレーション</li> <li>• 書き込み : オーケストレーション</li> </ul>
ポリシー : <ul style="list-style-type: none"> <li>• スケジュールの管理</li> <li>• API とオーケストレーション</li> </ul>	
管理 : <ul style="list-style-type: none"> <li>• ユーザとグループ</li> <li>• 統合</li> </ul>	



(注) [SCP User Configuration]、[Authentication Preferences]、および [Password Policy] などのレポートは、[Users and Groups] の下で **Operator** ロールに対して有効になります。



# ユーザアカウントの作成



(注) [Edit User] ダイアログボックスの [User Role] および [Login Name] フィールドは編集できません。

## 手順

- ステップ 1 メニューバーから、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2 [Users] タブをクリックします。
- ステップ 3 [Add] をクリックします。
- ステップ 4 [Add User] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[User Role] ドロップダウンリスト	[Group Admin]、[Operator]、または [System Admin] を選択します。
[User Group] ドロップダウンリスト	ユーザがアクセスできるようにするグループを選択します。すでに使用可能なグループを選択することも、新しいグループを追加することもできます。  (注) このフィールドは、ユーザロールとして [Group Admin] を選択している場合にのみ表示されます。
[Login Name] フィールド	ユーザのログイン名。
[Password] フィールド	ユーザのパスワード。ユーザに対して Lightweight Directory Access Protocol (LDAP) 認証が設定されている場合、パスワードはローカルサーバではなく、LDAP サーバでのみ検証されます。
[Confirm Password] フィールド	前のフィールドと同じパスワードを入力します。
[User Contact Email] フィールド	電子メールアドレス。
[First Name] フィールド	(オプション) ユーザの名。
[Last Name] フィールド	(オプション) ユーザの姓。
[Phone] フィールド	(オプション) ユーザの電話番号。
[Address] フィールド	(オプション) ユーザの物理アドレス。

ステップ 5 [Add] をクリックします。

ステップ 6 [OK] をクリックします。

## オンラインユーザの表示

現在オンラインであるユーザを表示するには、次の手順を実行します。

### 手順

ステップ 1 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [Current Online Users] タブをクリックします。

現在 Cisco IMC Supervisor にログインしているユーザのユーザ名、IP アドレス、セッション開始時刻などの詳細を確認できます。

## ユーザ ロールの追加

新しくインストールされた Cisco IMC Supervisor アプライアンスでは、デフォルトで、GroupAdmin ロールと Operator ロールを使用できます。グループ管理者のロールタイプは admin であるため、アクセス制限（メニュー設定とユーザ権限）の任意の組み合わせを使用して、既存の Operator ロールを必要に応じて変更できます。同様に、次の手順のように新しいロールを作成し、それらのロールにユーザを割り当てることもできます。

### 手順

ステップ 1 メニュー バーで、[Administration] > [System] を選択します。

ステップ 2 [User Roles] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add User Role] ダイアログボックスで、[User Role] ペインの次のフィールドに入力します。

フィールド	説明
[User Role] フィールド	ユーザ ロールの記述名。
[Role Type] ドロップダウン リスト	[Admin] を選択します。

フィールド	説明
[Description] フィールド	(オプション) ユーザ ロールの説明。

**ステップ 5** [Next] をクリックします。

**ステップ 6** [Menu Settings] ペインで、必要なメニュー オプションを選択します。  
メニュー オプションを選択するには、メニュー設定フィールドの横のチェックボックスをオンにします。

**ステップ 7** [Next] をクリックします。

**ステップ 8** [User Permissions] ペインで、必要な操作を選択します。  
操作を選択するには、操作の横のチェックボックスをオンにします。

**ステップ 9** [Submit] をクリックします。

**ステップ 10** 確認ダイアログボックスで、[OK] をクリックします。  
(注) ユーザ ロールを編集、複製、削除することもできます。

## ユーザ グループの追加

新しいユーザ グループを追加する場合は、次の手順を実行します。

### 手順

**ステップ 1** メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

**ステップ 2** [User Group] タブをクリックします。

**ステップ 3** [Add] をクリックします。

**ステップ 4** [Add User Group] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Name] フィールド	ユーザ グループの名前。
[Description] フィールド	(オプション) ユーザ グループの説明。
[Code] フィールド	(オプション) グループの短い名前またはコード名。
[Cost Center] フィールド	(オプション) コストセンターの名前または番号 (必要な場合)。この名前または番号は、グループが関連付けられているコストセンターを表します。

フィールド	説明
[Contact Email] フィールド	この電子メールは、必要に応じてサービスリクエストおよびリクエスト承認のステータスをグループ所有者に通知する目的で使用されます。
[First Name] フィールド	(オプション) 担当者の名。
[Last Name] フィールド	(オプション) 担当者の姓。
[Phone] フィールド	(オプション) 担当者の電話番号。
[Address] フィールド	(オプション) 担当者の住所。
[Group Share Policy] ドロップダウンリスト	(オプション) このグループのユーザのグループ共有ポリシーを選択します。  このドロップダウンリストは、グループ共有ポリシーを作成した場合にのみ表示されます。
[Allow Resource Assignment To Users] チェックボックス	(オプション) オンにすると、このグループのユーザは、そのユーザに割り当てられたリソースを持つことができ、これらのリソースを所有できます。また、これらのユーザは、グループに属するリソースを確認できます。しかし、ユーザ間でリソースを共有することはできません。

**ステップ 5** [Add] をクリックします。

**ステップ 6** [OK] をクリックします。

(注) これらのユーザグループを選択し、それらを表示、編集、削除、有効または無効にすることにより管理できます。[User Groups] タブからタグを管理することもできます。

## ユーザグループのブランディング

ユーザグループの Cisco IMC Supervisor アプリケーションをカスタマイズするには、次の手順を実行します。選択したグループに属するユーザがシステムにログインすると、カスタマイズされたページが表示されます。

## 手順

- ステップ 1** メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2** [User Group] タブをクリックします。
- ステップ 3** ユーザ グループを選択します。
- ステップ 4** [Branding] をクリックします。
- ステップ 5** [Group Branding] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Logo Image] チェックボックス	オンにすると、ロゴがアプリケーションの左上隅に表示されます。
[Application Labels] チェックボックス	オンにすると、アプリケーションのラベルがアプリケーションのヘッダー セクションに表示されます。
[URL Forwarding on Logout] チェックボックス	オンにすると、ユーザはログアウト時に指定された URL に転送されます。
[Custom Links] チェックボックス	オンにすると、カスタムリンクがアプリケーションの右上隅に表示されます。

- ステップ 6** [Submit] をクリックします。
- ステップ 7** [Submit Result] ダイアログボックスで [OK] をクリックします。

## グループ共有ポリシー

グループの共有ポリシーは、リソースのユーザと、ユーザが他のユーザと共有可能なものを、より詳細に制御できるようにします。このポリシーを使用すると、ユーザは、自分に現在割り当てられているリソースのみを表示可能にするか、またはそのユーザが属するすべてのグループに割り当てられているリソースを表示可能にすることができます。

グループの作成時に、グループの共有ポリシーを定義し、どのグループが読み取り/書き込み権限を持つかを決定できます。後にユーザがこのグループに追加されると、リソースに対するそのユーザのアクセス権は、グループに適用されるグループの共有ポリシーによって決定されます。

## グループ共有ポリシーの追加

ポリシーを追加して、ユーザ グループと共有するには、次の手順を実行します。

## 手順

- ステップ 1** メニューバーから、[Administration] > [Users and Groups] の順に選択します。
- ステップ 2** [Group Share Policy] タブをクリックします。
- ステップ 3** [Add] をクリックします。
- ステップ 4** [Add Group Share Policy] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Policy Name] フィールド	グループ共有ポリシーの名前。
[Policy Description] フィールド	ポリシーの説明。
[Select Groups] ドロップダウンリスト	作成したポリシーを共有するグループを選択します。

- ステップ 5** [Submit] をクリックします。
- ステップ 6** [Submit Result] ダイアログボックスで [OK] をクリックします。  
 (注) 既存のポリシーを選択して、表示、編集、削除、複製をすることもできます。



## 第 5 章

# サーバ検出、ラック グループ、およびラック アカウントの管理

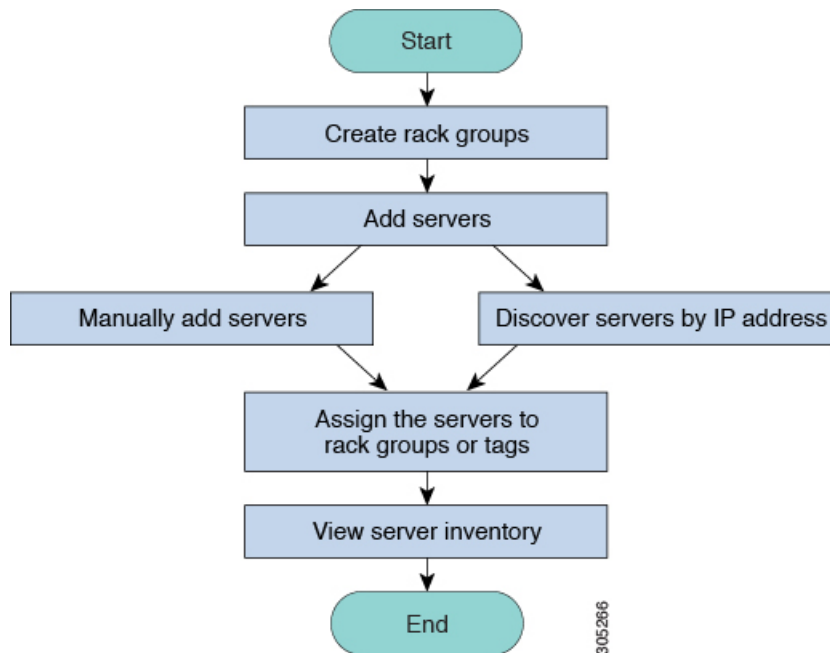
---

この章は、次の内容で構成されています。

- [概要, 51 ページ](#)
- [サーバの検出およびインポート, 52 ページ](#)
- [ラック グループの追加, 57 ページ](#)
- [ラック アカウントの追加, 58 ページ](#)
- [ラック アカウントまたはラック グループのインベントリの収集, 60 ページ](#)
- [ラック グループへのラック アカウントの割り当て, 61 ページ](#)
- [アカウント接続のテスト, 62 ページ](#)

## 概要

次の図は、Cisco IMC Supervisor でのグループの管理、ラック アカウントおよびサーバ検出に関するワークフローを示します。理想的には、ラック グループを作成し、サーバをこれらのラック グループに追加します。手動でのサーバの追加、またはサーバの検出ができます。これらのサーバの詳細インベントリを確認できます。



**使用例：**初めて Cisco IMC Supervisor をインストールする場合は、事前設定が一切されていないため、環境をセットアップする必要があります。管理に必要なシステムが世界中で何百もある可能性があります。手動で追加するか、または IP アドレスによって検出することで、これらのサーバを Cisco IMC Supervisor に導入できます。その前に、組織の要件に基づいて、これらのサーバの論理的なフィルタリングとタグングについて検討できます。たとえば、サーバを地域、建物番号、オペレーティングシステムなどでグループ化できます。タグ管理によって、Cisco IMC Supervisor に加わるサーバをより細かくグループ化できます。たとえば、Windows、Linux などを含むサーバにタグを追加して、オペレーティングシステムのラックグループ下でサーバをグループ化できます。また、既存のサーバにタグをオンザフライで追加する柔軟性もあります。

ラックグループまたはタグに名前を付ける決まった方法はありません。必要に合わせて自由に名前を決めることができます。ラックグループおよびタグの名前は入れ替えることができます。たとえば、Windows、Linux などという名前のラックグループがある場合に、オペレーティングシステムのタグ名の下にそのグループをタグ付けできます。

## サーバの検出およびインポート

ラックマウントサーバを自動的に検出して Cisco IMC Supervisor にインポートできます。次の項では、自動検出プロファイルの設定、自動検出の実行、および自動検出されたサーバのインポートなどのトピックについて取り上げます。

### 自動検出プロファイルの設定

Cisco IMC Supervisor がデバイスを検出するための基盤となる自動検出プロファイルを設定する必要があります。Cisco IMC Supervisor に設定できるプロファイル数に制限はありません。



自動検出プロファイルを追加または編集する場合は、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Systems] > [Physical Accounts] を選択します。
- ステップ 2** [Discovery Profiles] タブをクリックします。
- ステップ 3** [Add] をクリックします。
- ステップ 4** [Add Discovery Profile] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Profile Name] フィールド	プロファイルの記述名。
[Search Criteria] ドロップダウンリスト	ドロップダウン リストから [IP Address Range]、[Subnet Mask Range]、[IP Address CSV File]、または [IP Address List] を選択します。
[Starting IP] フィールド	有効な IP アドレス
[Ending IP] フィールド	有効な IP アドレス
[Use Credential Policy] チェックボックスがオンの場合	
[Credential Policy] ドロップダウンリスト	ポリシーをドロップダウン リストから選択するか、[+] アイコンをクリックして新しいポリシーを作成します。新しいポリシーの作成については、 <a href="#">クレデンシャルポリシーの作成</a> 、(92 ページ) を参照してください。
[Use Credential Policy] チェックボックスがオフの場合	
[User Name] フィールド	サーバのログイン名。
[Password] フィールド	サーバのログインパスワード
[Protocol] ドロップダウン リスト	リストから [https] または [http] を選択します。
[Port] フィールド	ポート番号を入力します。

フィールド	説明
<p>以下のフィールドは、[Search Criteria] で [IP Address Range]、[Subnet Mask Range]、および [IP Address List] を選択した場合のみ使用できます。</p> <p>(注) [IP Address CSV File] を選択した場合、これらのフィールドは CSV ファイルに次の形式で指定できます。サンプルの csv ファイルは、[File Template] をクリックすると使用できます。見出しなしで csv ファイルの最初の行からエントリを追加する必要があります。</p> <ul style="list-style-type: none"> <li>• &lt;ip&gt;</li> <li>• (オプション) &lt;description&gt;</li> <li>• (オプション) &lt;location&gt;</li> <li>• (オプション) &lt;contact&gt;</li> <li>• (オプション) &lt;rack group&gt;</li> <li>• (オプション) &lt;tag name:tag value&gt;;&lt;tag name:tag value&gt;</li> </ul> <p>(注)</p> <ul style="list-style-type: none"> <li>• Rack Group と Tags には、既存の値または新しい値を指定できます。これらのフィールドの指定は任意です。CSV ファイルに Rack Group の値を指定しない場合、Default Group が使用されます。</li> <li>• 現在の Cisco IMC Supervisor バージョンにアップグレードする場合は、既存の csv ファイルを、[Select a File] オプションを使用して新しい形式で作成した csv ファイルに置き換えます。</li> <li>• タグのタイプは STRING タイプのみです。</li> </ul>	
[Description] フィールド	サーバの説明を入力します。
[Contact] フィールド	サーバの連絡先の詳細を入力します。
[Location] フィールド	サーバのアドレスを入力します。
[Select Rack Group] ドロップダウンリストまたは [+] アイコン	ラックグループを選択するか、ラックグループを作成します。

**ステップ 5** [Submit] をクリックします。

**ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。

(注) また、プロファイルを変更、削除、表示することもできます。これらのタスクを実行するには、[Edit]、[Clear]、[Delete]、または [View] をクリックします。

## 自動検出の実行

システムが自動的にラックマウントサーバを検出して Cisco IMC Supervisor にインポートするようには、次の手順を実行します。

### はじめる前に

Cisco IMC Supervisor がデバイスを検出するための基盤となるプロファイルを設定する必要があります。

### 手順

- ステップ 1 メニューバーで、[Systems] > [Physical Accounts] を選択します。
- ステップ 2 [Discovered Devices] タブをクリックします。
- ステップ 3 [Discover] をクリックします。
- ステップ 4 [Discover Devices] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
[Select Profile] ドロップダウン リスト	[Select] をクリックして検出するプロファイルを選択します。検出するすべてのプロファイルのチェックボックスをオンにします。
[Schedule Later] チェックボックス	このチェックボックスをオンにして、後でサーバを自動検出するための既存のスケジュールを選択するか、または [+] をクリックして新しいスケジュールを作成します。スケジュール作成の詳細については、 <a href="#">スケジュールの作成</a> 、(143 ページ) を参照してください。[Policies] > [Manage Schedules] の順に移動して、スケジュールを選択し、[View Scheduled Tasks] をクリックしてスケジュールされたタスクを表示するか、または [Remove Scheduled Tasks] をクリックしてスケジュールされたタスクを削除できます。
[Schedule(s)] ドロップダウン リスト	[Schedule Later] チェックボックスを選択した場合、作成したスケジュールをドロップダウンリストから選択できます。  (注) また、このダイアログボックスから新しいスケジュールを作成することもできます。

**ステップ 5** [Submit] をクリックします。

**ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。

## サーバのインポート

自動検出を使用してサーバをインポートする場合は、次の手順を実行します。

### はじめる前に

- Cisco IMC Supervisor がデバイスを検出するための基盤となるプロファイルを設定する必要があります。
- すでに自動検出を実行済みです。

### 手順

**ステップ 1** メニューバーで、[Systems] > [Physical Accounts] を選択します。

**ステップ 2** [Discovered Devices] タブをクリックします。

**ステップ 3** [Import] をクリックします。

**ステップ 4** [Import Discovered Devices] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Select Device(s)] フィールド	[Select] をクリックしてインポートするデバイスを選択します。インポートするすべてのサーバのチェックボックスをオンにします。  (注) 特定のラックアカウントのインポートステータスがインポートされると、ステータスがインポートされ、そのラックアカウントはインポート用に表示されません。
[User Prefix]	ユーザのプレフィックスを入力します。

**ステップ 5** [Submit] をクリックします。

**ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。

- (注) 前のインポートプロセスが完了するのを待つことなく、検出されたデバイスを複数回インポートすることができます。

## 検出されたデバイスのプロパティの設定

検出されたデバイスのプロパティを設定する場合は、次の手順を実行します。

### はじめる前に

Cisco IMC Supervisor がデバイスを検出するための基盤となるプロファイルを設定する必要があります。

### 手順

- ステップ 1 メニューバーで、[Systems] > [Physical Accounts] を選択します。
- ステップ 2 [Discovered Devices] タブをクリックします。
- ステップ 3 [Discovered Devices] テーブルでデバイスを選択します。
- ステップ 4 [Set Properties] をクリックします。
- ステップ 5 [Set Properties] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
[Description] フィールド	サーバの説明を入力します。
[Contact] フィールド	サーバの連絡先の詳細を入力します。
[Location] フィールド	サーバのアドレスを入力します。
[Select Rack Group] ドロップダウン リストまたは [+] アイコン	ラックグループを選択するか、ラックグループを作成します。

- ステップ 6 [Submit] をクリックします。
- ステップ 7 確認ダイアログボックスで、[OK] をクリックします。

## ラックグループの追加

新しいラックグループを Cisco IMC Supervisor に追加する場合は、次の手順を実行します。デフォルトでは、システム定義のグループ [Default Group] を使用できます。

### はじめる前に

初めてログインする場合は、Cisco IMC Supervisor 用にライセンスが更新されていることを確認します。ライセンスをアップグレードするには、[ライセンスの更新](#)、(17 ページ) を参照してください。

## 手順

- ステップ 1** メニュー バーで、[Systems] > [Physical Accounts] を選択します。デフォルトでは、[Rack Group] タブが選択されます。
- ステップ 2** [Add] をクリックします。
- ステップ 3** [Create Rack Group] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Group Name] フィールド	ラック グループの記述名。
[Description] フィールド	(任意) ラック グループの説明。

- ステップ 4** [Create] をクリックします。
- ステップ 5** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## 次の作業

ラック グループに 1 つ以上のラック アカウントを追加します。

## ラック アカウントの追加

作成済みの既存のラック グループにラックマウント サーバを追加することも、新しいラック グループを作成してラックマウント サーバを追加することもできます。アカウントを追加すると、Cisco IMC Supervisor を使用してそのサーバを管理することができます。

既存のラック グループに新しいラックマウント サーバを追加する場合は、次の手順を実行します。

## はじめる前に

- 初めてログインする場合は、Cisco IMC Supervisor 用にライセンスがアップグレードされていることを確認します。ライセンスをアップグレードするには、[ライセンスの更新](#)、(17 ページ) を参照してください。
- ラック グループが存在することを確認します。



(注) システム提供のデフォルト グループまたは作成済みのラック グループの下にラック アカウントを追加できます。

- Cisco IMC Supervisor で XML API を有効にしていることを確認します。これによって、Cisco IMC Supervisor からラックマウントサーバを追加して管理できるようになります。

## 手順

- ステップ 1** メニューバーで、[System] > [Physical Accounts] を選択します。
- ステップ 2** [Rack Accounts] タブをクリックします。
- ステップ 3** [Add] をクリックします。
- ステップ 4** [Create Account] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Account Name] フィールド	ラックアカウントの記述名。
[Server IP] フィールド	ラックマウントサーバの IP アドレス、または Cisco UCS C3260 高密度ストレージラックサーバの仮想的な管理 IP アドレス。
[Description] フィールド	(オプション) ラックアカウントの説明。
[Use Credential Policy] チェックボックス	(オプション) すでにクレデンシャルポリシーを作成した場合は、このチェックボックスをオンにして、ドロップダウンリストからポリシーを選択します。
[Use Credential Policy] チェックボックスがオンの場合	
[Credential Policy] ドロップダウンリスト	ドロップダウンリストからポリシーを選択します。
[Use Credential Policy] チェックボックスがオフの場合	
[User Name] フィールド	ラックマウントサーバのログイン ID。
[Password] フィールド	ラックマウントサーバのログイン ID のパスワード。
[Protocol] ドロップダウンリスト	リストから [https] または [http] を選択します。
[Port] フィールド	選択したプロトコルに関連付けられたポート番号。

フィールド	説明
[Rack Group] ドロップダウン リストまたは [+] アイコン	リストからラックグループを選択するか、[+] をクリックしてラックグループを作成します。 ラックグループの作成の詳細については、 <a href="#">ラックグループの追加</a> 、(57 ページ) を参照してください。
[Contact] フィールド	(オプション) アカウントの連絡先電子メールアドレス。
[Location] フィールド	(オプション) アカウントの場所。

**ステップ 5** [Submit] をクリックします。

- (注)
- ラックアカウントを作成するための前のコマンドが完了するのを待つことなく、ラックアカウントを再び作成できます。
  - インベントリの編集、削除、収集、ラックサーバへのラックアカウントの割り当て、アカウント接続のテストを行うことができます。
  - 複数のラックアカウントを選択して削除することができます。インベントリ収集、障害ヘルス収集、ファームウェアアップグレード、ポリシーまたはプロファイルの適用、サーバ診断のタスクがアカウントのいずれかで実行されている場合は、アカウントを削除できません。

#### 次の作業

ラックサーバ接続をテストします。[アカウント接続のテスト](#)、(62 ページ) を参照してください。

## ラックアカウントまたはラックグループのインベントリの収集

ラックアカウントまたはラックグループのインベントリを収集するには、次の手順を実行します。

#### はじめる前に

ラックアカウントまたはラックグループがラックアカウントの下にすでに作成されています。



## 手順

- ステップ 1 メニューバーで、[Systems] > [Physical Accounts] を選択します。
- ステップ 2 [Rack Accounts] タブをクリックします。
- ステップ 3 ラックアカウントのリストが表示されます。
- ステップ 4 [Inventory] をクリックします。
- ステップ 5 [Collect Inventory for Account(s)] ダイアログボックスで、[Rack Group] または [Rack Account] を選択して、ドロップダウンリストからサーバを選択します。
- ステップ 6 サーバを選択するには [Select] をクリックします。
- ステップ 7 [Select] ダイアログボックスでサーバを選択して、[Select] をクリックします。  
(注) 選択対象となるラックグループまたはラックアカウントをフィルタに掛けるには、レポート上部にある検索バーを使用できます。
- ステップ 8 [Submit] をクリックします。
- ステップ 9 確認ダイアログボックスで、[OK] をクリックします。

# ラックグループへのラックアカウントの割り当て

ラックグループにサーバを割り当てるには、次の手順を実行します。

## はじめる前に

[Rack Accounts] で、ラックアカウントまたはサーバを作成しておきます。

## 手順

- ステップ 1 メニューバーで、[Systems] > [Physical Accounts] を選択します。
- ステップ 2 [Rack Accounts] タブをクリックします。
- ステップ 3 サーバの一覧が表示されます。
- ステップ 4 1 つ以上のサーバを選択して、[Assign Rack Group] をクリックします。
- ステップ 5 [Assign Rack Groups] ダイアログボックスで、サーバの割り当て先となるラックグループを選択します。  
(注) ラックグループを作成するには、[Assign Rack Group to selected server(s)] ドロップダウンリストの横にある [+] アイコンをクリックします。
- ステップ 6 [Submit] をクリックします。
- ステップ 7 確認ダイアログボックスで、[OK] をクリックします。

## アカウント接続のテスト

1つ以上のラックアカウントの接続をテストする場合は、次の手順を実行します。Cisco IMC Supervisorに追加されたすべての新しいアカウントに対して、この手順を実行することを推奨します。

### 手順

- 
- ステップ1 メニューバーで、[Systems] > [Physical Accounts] を選択します。
  - ステップ2 [Rack Accounts] タブをクリックします。
  - ステップ3 ラックアカウントのリストから、接続をテストするアカウントを選択します。
  - ステップ4 [Test Connection] をクリックします。  
(注) リストから少なくとも1つのラックアカウントを選択するまで、[Test Connection] ボタンは表示されません。
  - ステップ5 [Test Connection] ダイアログボックスで、[Submit] をクリックします。  
接続のテストには数分かかる場合があります。
  - ステップ6 確認ダイアログボックスで、[OK] をクリックします。  
接続ステータスと、成功または失敗の理由が [Rack Accounts] ページに表示されます。
-



## 第 6 章

# インベントリ データおよび障害の表示

この章は、次の内容で構成されています。

- [ラックマウント サーバの詳細の表示, 63 ページ](#)
- [ラック マウント サーバの障害の詳細の表示, 66 ページ](#)
- [ラック グループのサマリー レポート, 66 ページ](#)
- [サーバ障害に関する電子メールアラート ルールの追加, 67 ページ](#)

## ラックマウント サーバの詳細の表示

ラックマウント サーバの詳細（サーバで使用されているメモリ、CPU、PSU など）を表示する場合は、次の手順を実行します。



- (注) 左側のペインで [Rack Groups] をクリックし、次の手順を実行してラックマウント サーバの詳細を表示することもできます。

### はじめる前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

### 手順

- ステップ 1** メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで、[Rack Groups] を展開し、サーバを含むラック グループを選択します。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。
- ステップ 4** リストにあるサーバをダブルクリックして詳細を表示するか、リストにあるサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

(注) リストからサーバを選択するまでは、右端に下向き矢印は表示されません。

ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
[Summary]	ラック アカウントの概要。
[CPU]	サーバで使用されている CPU の詳細。
[Memory]	サーバで使用されているメモリの詳細。
[PSUs]	サーバで使用されている電源装置の詳細。 (注) Cisco UCS C3260 高密度ストレージ ラック サーバの場合は該当しません。
[PCI Adapters]	サーバで使用されている PCI アダプタの詳細。
[VIC Adapters]	サーバで使用されている VIC アダプタの詳細。 リストにある任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] や [VM FEXs] などの情報が表示されます。
[Network Adapters]	サーバで使用されているネットワーク アダプタの詳細。 リストされている任意のネットワーク アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] の情報が表示されます。
[Storage Adapters]	サーバで使用されているストレージ アダプタの詳細。 リストにある任意のストレージアダプタを選択して [View Details] をクリックすると、[Controller Info] や [Physical Drives] などの情報が表示されます。
[FlexFlash Adapters]	サーバで使用されている FlexFlash アダプタの詳細。 リストにある任意の FlexFlash アダプタを選択して [View Details] をクリックすると、[Controller Info] や [Physical Drives] などの情報が表示されます。Cisco IMC Supervisor を旧バージョンからアップグレードしている場合、FlexFlash の詳細をレポートに表示するには [Systems] > [Physical Accounts] > [Rack Accounts] > [Inventory] に移動してインベントリを実行するか、定期的なインベントリが実行されるのを待つ必要があります。 (注) Cisco UCS C3260 高密度ストレージ ラック サーバの場合は該当しません。
[Communication]	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルの情報。
[Remote Presence]	vKVM、Serial over LAN、vMedia の詳細。

タブ	説明
[Faults]	サーバで記録された障害の詳細。
[Users]	ユーザの詳細。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[Cisco IMC Log]	サーバの Cisco IMC ログの詳細。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[System Event Log]	サーバ ログの詳細。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[TPM]	TPM インベントリに関する情報。
[BIOS]	サーバの BIOS 設定とブート順序に関する詳細。 サーバを選択して、[View BIOS Settings]、[View Boot Settings]、または [View Boot Order] をクリックしてください。
[Fault History]	サーバで発生した障害の履歴情報。
[Tech Support]	ファイル名、宛先タイプ、アップロードのステータスなどのテクニカルサポート ログ ファイルに関する詳細は、[Tech Support] テーブルに表示されます。 リモート サーバまたはローカルの Cisco IMC Supervisor アプライアンスにテクニカルサポート ログ ファイルをエクスポートするオプションがあります。エクスポートの詳細については、 <a href="#">リモートサーバへのテクニカルサポート データのエクスポート</a> 、(85 ページ) を参照してください。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[Associated Hardware Profiles]	ハードウェア プロファイルに関連付けられているポリシーの詳細。

**ステップ 5** 右端の [Back] ボタンをクリックして前のウィンドウに戻ります。

## ラック マウント サーバの障害の詳細の表示

問題の原因や問題解決のための推奨手順など、ラック マウント サーバの障害の詳細を表示する場合は、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

### 手順

- 
- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。
- ステップ 3** 右側のペインで、[Faults] タブを選択します。
- ステップ 4** リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。  
 (注) リストからサーバを選択するまでは、右端に下向き矢印は表示されませ  
 ん。  
 ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
[Explanation]	問題の原因の要約。
[Recommendation]	問題を解決する手順。

- ステップ 5** [Fault Details] ウィンドウで [Close] をクリックすると、前のウィンドウに戻ります。
- 

## ラック グループのサマリー レポート

[Inventory and Fault Status for Rack Groups] ページは、左右 2 つのセクションに分かれています。左側のペインにはラック グループのリストが表示されます。[Rack Groups] の見出しがデフォルトグループを含む左側のペインで選択されている場合、サマリー レポートは、次のレポートが表示される右側のペインで使用することができます。

- [Faults] : 選択されたラック グループに対し、全体の障害の数を表します。障害の数は、[Critical]、[Major]、[Warnings]、[Minor]、[Info] などの重大度に基づいて分類されます。
- [Server Health] : サーバ全体のヘルス ステータスを表します。サーバ全体のヘルス ステータスは、[Good]、[Memory Test In Progress]、[Moderate Fault]、[Severe Fault] などの状態のいずれかになります。



(注) [Moderate Fault] と [Severe Fault] は、重大度が [Major] および [Critical] となっている障害とそれぞれ相互に関連します。しかし、サーバのヘルス ステータスは CIMC によって報告されるステータスに基づいて決定され、上記の障害の重要度対して、常に直接的にマッピングされるわけではないことに注意してください。障害のタイプや関連コンポーネントなどの他の要素がサーバ全体のヘルス ステータスに影響します。

- [Firmware Versions] : 選択されたラック グループに対し、そのファームウェア バージョンで管理されているサーバの全体的な数を表します。
- [Server Models] : 選択されたラック グループに対し、そのモデルで管理されているサーバの全体的な数を表します。
- [Power State] : 選択されたラック グループに対し、その電源状態で管理されているサーバの全体的な数を表します。電源の状態は [On] または [Off] のいずれかです。
- [Server Connection Status] : 選択されたラック グループに対し、その接続ステータスをもつサーバの全体的な数を表します。接続ステータスは [Success] または [Failed] のいずれかです。

## サーバ障害に関する電子メールアラートルールの追加

1 つ以上の電子メールルールを作成できます。各ルールでは、指定した条件に一致する障害が定期的な検査で見つかり、電子メールアラートが送信されます。このような障害に関する電子メールアラートを受信するには、次の手順を実行します。

### 手順

**ステップ 1** メニューバーで、[Administration] > [System] を選択します。

**ステップ 2** [Email Alert Rules] タブをクリックします。

(注) [Email Alert Rules] テーブルには、電子メールアラートのルール名、アラート範囲、アラートルールで選択されたサーバとサーバグループなどのアラートルールの詳細が表示されます。

**ステップ 3** [Add] をクリックします。

**ステップ 4** [Add Email Alert Rule] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Name]	ルールの一意の名前を入力します。

フィールド	説明
[Alert Scope]	<p>任意のサーバで検出された新しい障害に関するすべてのシステムレベルのアラートを受信するには [System] を選択します。特定のラックグループの一部であるサーバで検出された新しい障害に関する電子メールアラートを受信するには [ServerGroup] を選択します。特定のサーバで検出された新しい障害に関する電子メールアラートを受信するには [Server] を選択します。</p>
[Server Groups]	<p>アラートレベルで [ServerGroup] を選択した場合、このオプションが表示されます。</p> <ol style="list-style-type: none"> <li>1 [Select] をクリックします。</li> <li>2 [Select] ダイアログボックスで1つ以上のラックサーバグループにチェックマークを付けて、[Select] をクリックします。電子メールアラートの送信対象となる選択されたサーバグループの名前が、このフィールドの横にリストされます。</li> </ol>
[Servers]	<p>アラートレベルで [Server] を選択した場合、このオプションが表示されます。</p> <ol style="list-style-type: none"> <li>1 [Select] をクリックします。</li> <li>2 [Select] ダイアログボックスで1つ以上のサーバにチェックマークを付けて、[Select] をクリックします。電子メールアラートの送信対象となる選択されたサーバ名が、このフィールドの横にリストされます。</li> </ol>
[Email Addresses] フィールド	<p>電子メールアラートの対象受信者の電子メールアドレス。複数の電子メールアドレスをカンマで区切って入力できます。</p>



フィールド	説明
[Severity]	<p>[Email Addresses] フィールドに設定された電子メールアドレスに電子メールアラートを送信する対象となる障害重大度レベルを選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1 [Select...] をクリックします。</li> <li>2 リストから1つ以上の重大度レベルにチェックマークを付けて、[Select] をクリックします。</li> </ol> <p>(注) 選択した値が [Select...] ボタンの横に表示されます。</p>
[Rule Enabled] チェックボックス	このチェックボックスをオンにして、設定された電子メールアドレスへの電子メールアラートを有効にします。

- (注)
- 電子メールアラートのルールを修正と削除ができます。[Edit] および [Delete] オプションは、ルールを選択した場合にのみ表示されます。[Edit] をクリックし、表示されているフィールドを必要に応じて変更するか、[Delete] をクリックして、削除することを確認します。
  - 複数のルールを同時に選択して [Delete] をクリックすると、それらを削除できます。
  - 送信される電子メールアラートの数は、作成したルールの数に基づいています。
  - 1.0 または 1.0.0.1 でシステム レベルルールが存在する場合、1.1 にアップグレードすると、デフォルトのルールの名前が [system-default] として追加されたことを確認できます。このグループの [Alert Level] フィールドを変更することはできませんが、このシステム レベルルールを削除することは可能です。





## 第 7 章

# ラック サーバの管理

---

この章は、次の内容で構成されています。

- [ラックマウント サーバの詳細の表示, 71 ページ](#)
- [ラック マウント サーバの障害の詳細の表示, 74 ページ](#)
- [ラック マウント サーバの電源オン/オフ, 75 ページ](#)
- [ラックマウント サーバのシャットダウン, 75 ページ](#)
- [ラックマウント サーバのハードリセットの実行, 76 ページ](#)
- [ラック マウント サーバの電源再投入の実行, 77 ページ](#)
- [ラックマウント サーバの KVM コンソールの起動, 77 ページ](#)
- [ラックマウント サーバの GUI の起動, 78 ページ](#)
- [ラックマウント サーバのロケータ LED の設定, 79 ページ](#)
- [ラックマウント サーバのラベルの設定, 80 ページ](#)
- [ラックマウント サーバのタグの管理, 80 ページ](#)
- [ラックマウント サーバのタグの追加, 84 ページ](#)
- [リモート サーバへのテクニカル サポート データのエクスポート, 85 ページ](#)
- [SEL のクリア, 87 ページ](#)
- [システム タスクの管理, 87 ページ](#)

## ラックマウント サーバの詳細の表示

ラックマウント サーバの詳細（サーバで使用されているメモリ、CPU、PSU など）を表示する場合は、次の手順を実行します。



(注) 左側のペインで [Rack Groups] をクリックし、次の手順を実行してラックマウント サーバの詳細を表示することもできます。

### はじめる前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

### 手順

- ステップ 1** メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで、[Rack Groups] を展開し、サーバを含むラック グループを選択します。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。
- ステップ 4** リストにあるサーバをダブルクリックして詳細を表示するか、リストにあるサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。
- (注) リストからサーバを選択するまでは、右端に下向き矢印は表示されません。
- ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
[Summary]	ラック アカウントの概要。
[CPU]	サーバで使用されている CPU の詳細。
[Memory]	サーバで使用されているメモリの詳細。
[PSUs]	サーバで使用されている電源装置の詳細。 (注) Cisco UCS C3260 高密度ストレージラックサーバの場合は該当しません。
[PCI Adapters]	サーバで使用されている PCI アダプタの詳細。
[VIC Adapters]	サーバで使用されている VIC アダプタの詳細。 リストにある任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] や [VM FEXs] などの情報が表示されます。
[Network Adapters]	サーバで使用されているネットワーク アダプタの詳細。 リストされている任意のネットワーク アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] の情報が表示されます。

タブ	説明
[Storage Adapters]	サーバで使用されているストレージアダプタの詳細。 リストにある任意のストレージアダプタを選択して [View Details] をクリックすると、[Controller Info] や [Physical Drives] などの情報が表示されます。
[FlexFlash Adapters]	サーバで使用されている FlexFlash アダプタの詳細。 リストにある任意の FlexFlash アダプタを選択して [View Details] をクリックすると、[Controller Info] や [Physical Drives] などの情報が表示されます。 Cisco IMC Supervisor を旧バージョンからアップグレードしている場合、FlexFlash の詳細をレポートに表示するには [Systems] > [Physical Accounts] > [Rack Accounts] > [Inventory] に移動してインベントリを実行するか、定期的なインベントリが実行されるのを待つ必要があります。  (注) Cisco UCS C3260 高密度ストレージラックサーバの場合は該当しません。
[Communication]	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルの情報。
[Remote Presence]	vKVM、Serial over LAN、vMedia の詳細。
[Faults]	サーバで記録された障害の詳細。
[Users]	ユーザの詳細。  (注) Cisco UCS C3260 高密度ストレージラックサーバの場合は該当しません。
[Cisco IMC Log]	サーバの Cisco IMC ログの詳細。  (注) Cisco UCS C3260 高密度ストレージラックサーバの場合は該当しません。
[System Event Log]	サーバログの詳細。  (注) Cisco UCS C3260 高密度ストレージラックサーバの場合は該当しません。
[TPM]	TPM インベントリに関する情報。
[BIOS]	サーバの BIOS 設定とブート順序に関する詳細。 サーバを選択して、[View BIOS Settings]、[View Boot Settings]、または [View Boot Order] をクリックしてください。
[Fault History]	サーバで発生した障害の履歴情報。

タブ	説明
[Tech Support]	<p>ファイル名、宛先タイプ、アップロードのステータスなどのテクニカルサポート ログ ファイルに関する詳細は、[Tech Support] テーブルに表示されます。</p> <p>リモート サーバまたはローカルの Cisco IMC Supervisor アプライアンスにテクニカル サポート ログ ファイルをエクスポートするオプションがあります。エクスポートの詳細については、<a href="#">リモートサーバへのテクニカルサポート データのエクスポート</a>、(85 ページ) を参照してください。</p> <p>(注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。</p>
[Associated Hardware Profiles]	ハードウェア プロファイルに関連付けられているポリシーの詳細。

**ステップ 5** 右端の [Back] ボタンをクリックして前のウィンドウに戻ります。

## ラック マウント サーバの障害の詳細の表示

問題の原因や問題解決のための推奨手順など、ラック マウントサーバの障害の詳細を表示する場合は、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

### 手順

- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。
- ステップ 3** 右側のペインで、[Faults] タブを選択します。
- ステップ 4** リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。  
(注) リストからサーバを選択するまでは、右端に下向き矢印は表示されません。  
ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
[Explanation]	問題の原因の要約。

タブ	説明
[Recommendation]	問題を解決する手順。

**ステップ 5** [Fault Details] ウィンドウで [Close] をクリックすると、前のウィンドウに戻ります。

## ラック マウント サーバの電源オン/オフ

ラック マウント サーバの電源をオンまたはオフにする場合は、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

### 手順

- ステップ 1** メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラック グループを選択することもできます。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブ グループを選択することもできます。
- ステップ 4** サーバのリストから、電源をオンまたはオフにするサーバを選択します。  
(注) 複数のラック サーバを選択することもできます。
- ステップ 5** [Power ON] または [Power OFF] をクリックするか、右クリックしてオプションを選択します。  
(注) リストからサーバを選択するまでは、[Power On] および [Power Off] ボタンは表示されません。
- ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。  
(注) サーバの電源がオンまたはオフになったことを示すメッセージが表示されます。また、このメッセージは、いずれかのサーバの電源オン/オフを実行できなかったかどうかを示します。少し時間が経過した後でテーブルを更新すると、現在の電源状態が反映されます。

## ラックマウント サーバのシャットダウン

ラックマウント サーバをシャットダウンする場合は、次の手順を実行します。



(注) 複数のラックサーバを選択することもできます。

### はじめる前に

サーバはすでに、ラックアカウントとしてラックグループに追加されています。

### 手順

- 
- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラックグループを選択することもできます。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブグループを選択することもできます。
- ステップ 4** リストからサーバを選択します。
- ステップ 5** [Shut Down] をクリックするか、右クリックしてオプションを選択します。  
(注) リストからサーバを選択するまでは、[Shut Down] ボタンは表示されません。また、右端にある下矢印をクリックしてオプションを選択することもできます。
- ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。
- 

## ラックマウントサーバのハードリセットの実行

サーバをリセットするには、次の手順を実行します。



(注) 複数のラックサーバを選択することもできます。

### はじめる前に

サーバはすでに、ラックアカウントとしてラックグループに追加されています。

### 手順

- 
- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラックグループを選択することもできます。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。



- (注) また、左側のペインの [Rack Groups] で、サブグループを選択することもできます。
- ステップ 4** リストからサーバを選択します。
- ステップ 5** [Hard Reset] をクリックします。
- (注) リストからサーバを選択するまでは、[Hard Reset] ボタンは表示されません。また、右端にある下矢印をクリックしてオプションを選択することもできます。
- ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。

## ラック マウント サーバの電源再投入の実行

ラック マウント サーバの電源を 1 サイクルでオンまたはオフにするには、次の手順を実行します。



- (注) 複数のラック サーバを選択することもできます。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

### 手順

- ステップ 1** メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。
- (注) [Rack Groups] を展開し、サーバを含むラック グループを選択することもできます。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。
- (注) また、左側のペインの [Rack Groups] で、サブグループを選択することもできます。
- ステップ 4** リストからサーバを選択します。
- ステップ 5** [Power Cycle] をクリックします。
- (注) リストからサーバを選択するまでは、[Power Cycle] ボタンは表示されません。また、右端にある下矢印をクリックしてオプションを選択することもできます。
- ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。

## ラックマウント サーバの KVM コンソールの起動

*kvm.jnlp* ファイルをダウンロードし、KVM コンソールを開くには、次の手順を実行します。

### はじめる前に

- サーバがラック アカウントとしてラック グループに追加されていることを確認します。
- KVM 機能が機能するために必要な有効な Java Runtime Environment (JRE) がインストールされていることを確認します。

### 手順

- 
- ステップ 1** メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラック グループを選択することもできます。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブ グループを選択することもできます。
- ステップ 4** リストからサーバを選択します。
- ステップ 5** [KVM Console] をクリックします。  
(注) リストから少なくとも 1 台のサーバを選択するまでは、[KVM Console] ボタンは表示されません。KVM コンソールを起動するサーバは最大 5 台選択できます。
- ステップ 6** [Submit] をクリックします。  
Cisco IMC Supervisor によって *kvm.jnlp* ファイルがダウンロードされます。
- ステップ 7** ダウンロード フォルダ内の *kvm.jnlp* ファイルをダブルクリックします。  
[KVM Console] が別ウィンドウで開きます。  
(注) 別のウィンドウで開く *launcher.jsp* ファイルに、選択したサーバのリストが表示されます。KVM コンソールが正常に起動しているか確認することもできます。
- 

## ラックマウント サーバの GUI の起動

別のブラウザから Cisco IMC Supervisor GUI を起動するには、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

### 手順

- 
- ステップ 1** メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラック グループを選択することもできます。

- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブグループを選択することもできます。
- ステップ 4** リストからサーバを選択します。
- ステップ 5** [Launch GUI] をクリックします。  
(注) リストからサーバを選択するまでは、[Launch GUI] ボタンは表示されません。
- ステップ 6** [Launch GUI] ダイアログボックスで、[Submit] をクリックします。  
サーバの GUI が別のブラウザで起動します。

## ラックマウントサーバのロケータ LED の設定

サーバロケータ LED を使用すると、データセンター内の多数のサーバ間で特定のサーバを識別できます。LED をオン/オフに設定するには、次の手順を実行します。



- (注) 複数のラックサーバを選択することもできます。

### はじめる前に

サーバはすでに、ラックアカウントとしてラックグループに追加されています。

### 手順

- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラックグループを選択することもできます。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブグループを選択することもできます。
- ステップ 4** リストからサーバを選択します。
- ステップ 5** [Locator LED] をクリックします。  
(注) リストからサーバを選択するまでは、[Locator LED] ボタンは表示されません。
- ステップ 6** [Turn] ドロップダウンリストから、[ON] または [OFF] を選択します。
- ステップ 7** [Submit] をクリックします。
- ステップ 8** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## ラックマウントサーバのラベルの設定

サーバにラベル名を設定することで、サーバの分類に役立ちます。これによって、必要なサーバの検索、表示、比較がしやすくなります。ラックマウントサーバにラベルを設定するには、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

### 手順

- 
- ステップ 1 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
  - ステップ 2 左側のペインで [Rack Groups] を選択します。  
(注) [Rack Groups] を展開し、サーバを含むラック グループを選択することもできます。
  - ステップ 3 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブ グループを選択することもできます。
  - ステップ 4 リストからサーバを選択します。
  - ステップ 5 [Set Label] をクリックします。  
(注) リストからサーバを選択するまでは、[Set Label] ボタンは表示されません。
  - ステップ 6 新しいラベルを入力します。
  - ステップ 7 [Submit] をクリックします。
  - ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## ラックマウントサーバのタグの管理

タギングは、リソースグループまたはラックサーバなどのオブジェクトにラベルを割り当てるために使用されます。タグは、ラックの位置、担当サポートグループ、目的、またはオペレーティングシステムなどの情報を提供するために使用できます。タグを追加または変更するには、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

## 手順

- 
- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで、[Rack Groups] を展開し、サーバを含むラックグループを選択します。
- ステップ 3** 右側のペインで、[Rack Servers] または [Chassis] タブを選択します。  
(注) 左側のペインの [Rack Groups] では、任意のサブグループを選択できません。
- ステップ 4** [Manage Tags] をクリックします。  
(注) リストからラックマウントサーバまたは UCS 3260 サーバを選択するまでは、[Manage Tags] ボタンは表示されません。
- ステップ 5** [+] をクリックして、[Manage Tags] テーブルにエントリを追加します。
- ステップ 6** [Add Entry to Tag] ダイアログボックスで、次のように入力します。

フィールド	説明
[Tag Name]	

フィールド	説明
	<p>ドロップダウンリストからタグ名を選択して [Submit] をクリックするか、新しいタグを作成します。</p> <ol style="list-style-type: none"> <li>1 [+] アイコンをクリックします。</li> <li>2 [Create Tag] ウィンドウで、次の手順を実行します。 <ol style="list-style-type: none"> <li>a [Name] フィールドに、タグを記述する名前を入力します。</li> <li>b [Description] フィールドに、タグの説明を入力します。</li> <li>c [Type] フィールドで、ドロップダウンリストから文字列または整数を選択します。</li> <li>d [Possible Tag Values] フィールドで、可能なタグ値を入力します。</li> <li>e [Next] をクリックします。</li> <li>f [+] アイコンをクリックして、新しいカテゴリを追加します。</li> </ol> </li> <li>3 [Add Entry to Entities] ウィンドウで、[Category] ドロップダウンリストからカテゴリを選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• [Physical_Compute] カテゴリの場合、ラックサーバのタグエンティティが作成されます。</li> <li>• [Administration] カテゴリの場合、ユーザ用のタグエンティティが作成されます。</li> </ul> <p>(注) シャーシのタグを追加することもできます。シャーシのタグの追加方法の詳細については、<a href="#">Cisco UCS C3260 ラックサーバのタグの追加 (157 ページ)</a> を参照してください。</p> </li> <li>4 [Rack Servers] または [Chassis] チェックボックスをオンにします。</li> </ol>

フィールド	説明
	<p>5 [Submit] をクリックします。</p> <p>(注) タグは、タグ付け可能なエンティティの設定に応じてそれぞれのカテゴリの下に表示されます。</p> <p>6 確認ダイアログボックスで、[OK] をクリックします。</p>
[Tag Value]	ドロップダウンリストからタグ値を選択します。

ステップ7 [Submit] をクリックします。

ステップ8 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ9 [Manage Tags] ダイアログボックスでタグを選択し、[Edit] アイコンをクリックしてタグを編集できます。

ステップ10 タグ名とタグ値を選択して、タグを変更します。

ステップ11 [Submit] をクリックします。

ステップ12 [Submit Result] ダイアログボックスで、[OK] をクリックします。

## ラックマウントサーバのタグの追加

タグgingは、リソースグループまたはラックサーバなどのオブジェクトにラベルを割り当てるために使用されます。タグは、ラックの位置、担当サポートグループ、目的、オペレーティングシステムなどの情報を提供するために使用できます。ラックマウントサーバにタグを追加するには、次の手順を実行します。

### はじめる前に

サーバはすでに、ラックアカウントとしてラックグループに追加されています。



(注) 複数のラックサーバを選択することもできます。



## 手順

- 
- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで、[Rack Groups] を展開し、サーバを含むラックグループを選択します。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。  
(注) また、左側のペインの [Rack Groups] で、サブグループを選択することもできます。
- ステップ 4** [Add Tags] をクリックします。  
(注) リストからサーバを選択するまでは、[Add Tags] ボタンは表示されません。
- ステップ 5** ドロップダウンリストから [Tag Name] を選択します。
- ステップ 6** ドロップダウンリストから [Tag Value] を選択します。
- ステップ 7** [+]アイコンをクリックして、新しいタグを作成します。タグの作成については、[ラックマウントサーバのタグの管理](#)、(80 ページ) を参照してください。  
(注) また、タグの詳細を複製、編集、削除、表示することもできます。
- 

# リモートサーバへのテクニカルサポートデータのエクスポート

指定したサーバにテクニカルサポートファイルをアップロードするには、次の手順を実行します。



- 
- (注) テクニカルサポートのエクスポートオプションでは、[Rack Servers] タブからの Cisco UCS C3260 高密度ストレージラックサーバのエクスポートはサポートされていません。
-

## 手順

- ステップ 1** メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2** 左側のペインで [Rack Groups] を選択します。
- ステップ 3** 右側のペインで、[Rack Servers] タブを選択します。
- ステップ 4** リストにあるラックマウントサーバをダブルクリックして詳細を表示するか、リストにあるラックマウントサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。
- ステップ 5** [Tech Support] タブをクリックします。
- ステップ 6** [Create Tech Support] をクリックします。
- ステップ 7** [Create Tech Support] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Destination Type] ドロップダウンリスト	リモートサーバまたはローカルの Cisco IMC Supervisor アプリケーションにファイルをエクスポートできます。[REMOTE] または [LOCAL] を選択します。
[Network Type] ドロップダウンリスト	ネットワーク タイプ。次のいずれかになります。 <ul style="list-style-type: none"> <li>• [SCP]</li> <li>• [SFTP]</li> <li>• [FTP]</li> <li>• [TFTP]</li> </ul>
[Server IP/Hostname] フィールド	サポートデータファイルを保存する必要があるサーバの IP アドレスまたはホスト名。[Network Type] ドロップダウンリストの設定によって、このフィールドの名前が異なります。
[Path and Filename] フィールド	ファイルをリモートサーバにエクスポートする際に必要なパスおよびファイル名。
[Username]	システムがリモートサーバへのログインに使用する必要があるユーザ名。ネットワークタイプが TFTP の場合、このフィールドは適用されません。
[Password]	リモートサーバのユーザ名のパスワード。ネットワークタイプが TFTP の場合、このフィールドは適用されません。

- ステップ 8** [Submit] をクリックします。

- (注)
- 選択してダウンロードできるテクニカル サポート ファイルは、[Destination Type] として [LOCAL] を選択して作成されたものだけです。
  - 既存のテクニカル サポート ファイルを選択し、Cisco IMC Supervisor アプライアンス内に保存されているファイルのみをダウンロードできます。特定のファイルを選択し、[Download] をクリックします。<hostname>\_<timestamp>.tar.gz ファイルが作成されます。

## SEL のクリア

システム イベント ログ (SEL) は、問題のトラブルシューティングに使用できるほとんどのサーバ関連イベントを記録します。SEL ログをクリアするには、次の手順を実行します。

### 手順

- ステップ 1 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2 左側のペインで [Rack Groups] を選択します。
- ステップ 3 右側のペインで、[Rack Servers] タブを選択します。
- ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。
- ステップ 5 [System Event Log] タブをクリックします。
- ステップ 6 [Clear IMC SEL Log] をクリックします。
- ステップ 7 (任意) [Clear IMC SEL Logs] ダイアログボックスで、[Delete historical logs from Cisco IMC Supervisor] チェックボックスをオンにします。  
このオプションを選択すると、Cisco IMC Supervisor GUI からシステム イベント ログがクリアされます。
- ステップ 8 [Submit] をクリックします。

## システム タスクの管理

[System Tasks] タブには、現在 Cisco IMC Supervisor で利用可能なすべてのシステム タスクが表示されます。ただし、このシステム タスクのリストは、Cisco IMC Supervisor で作成したアカウントのタイプにリンクされています。たとえば、初めてログインした場合は、一連の汎用システム関連のタスクだけがこのページに表示されます。ラック アカウントや Cisco IMC Supervisor アカウントなどのアカウントを追加した時点から、これらのアカウントに関連するシステムのタスクがこのページに読み込まれます。

左側のペインでタスクを展開し、消去、ラックサーバ、ユーザ、グループタスクなどの個々のタスクを選択して、それらを管理します。

アプライアンスで実行しているプロセスまたはタスクが複数ある状況において、システムタスクの無効化を選択することができます。無効にすると、手動で有効にするまで、システムタスクは実行されません。これは他のレポートに入力されるデータに影響します。たとえば、インベントリ収集のシステムタスクを無効にすると、このデータが必要なレポートに正確なデータが表示されない場合があります。この場合、インベントリ収集プロセスを手動で実行するか、またはシステムタスクを有効にする必要があります。



(注) システムタスクの編集は推奨されません。

### 手順

**ステップ 1** メニューバーで、[Administration] > [System] を選択します。

**ステップ 2** [System Tasks] タブをクリックします。

**ステップ 3** リストからタスクを選択し、[Manage Task] をクリックします。

**ステップ 4** [Manage Task] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Task Execution] ドロップダウンリスト	(オプション) [Enable] または [Disable] を選択します。
[System Task Policy] ドロップダウンリスト	次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> <li>• default-system-task-policy</li> <li>• local-run-policy</li> </ul>
[Hours] ドロップダウンリスト	タスクを実行する間隔を時間単位で選択します。

**ステップ 5** [Submit] をクリックします。

**ステップ 6** [OK] をクリックします。

## タスクの実行

各タスクは、ユーザが定義した間隔で実行するようにスケジュールされます。ただし、これを上書きして手動で実行することができます。手動で実行したタスクは、再度頻度カラムの定義に従って実行するようにスケジュールされます。システムタスクを手動で実行する場合は、次の手順を実行します。

## 手順

---

- ステップ 1 メニューバーで、[Administration] > [System] を選択します。
  - ステップ 2 [System Tasks] タブをクリックします。
  - ステップ 3 テーブルからシステム タスクを選択します。
  - ステップ 4 [Run Now] をクリックします。
  - ステップ 5 [Submit] をクリックします。
  - ステップ 6 [OK] をクリックします。
-





## 第 8 章

# ポリシーとプロファイルの管理

この章は、次の内容で構成されています。

- [クレデンシャル ポリシー, 91 ページ](#)
- [ハードウェア ポリシー, 92 ページ](#)
- [ハードウェア プロファイル, 128 ページ](#)
- [タグ ライブラリ, 133 ページ](#)

## クレデンシャル ポリシー

ポリシーは、システムまたはネットワーク リソースへのアクセスを制御するルールのセットから成ります。クレデンシャルポリシーは、ユーザアカウントのパスワードの要件とアカウントロックアウトを定義します。ユーザアカウントに割り当てられたクレデンシャルポリシーは、Cisco IMC Supervisor での認証プロセスを制御します。クレデンシャルポリシーを追加した後、新しいポリシーをクレデンシャルタイプのデフォルトのポリシーとして割り当てるか、または個々のアプリケーションに割り当てることができます。

[Credential Policies] ページには、次の詳細が表示されます。

フィールド	説明
[Policy Name]	ポリシーのユーザ定義名。
[Description]	ポリシーのユーザ定義の簡単な説明。
[Username]	シスコ ユーザ名。
[Protocol]	ポリシーが準拠するプロトコル。
[Port]	ポリシーのポート。

このページから、ポリシーの追加、編集、削除など、さまざまなタスクを実行できます。クレデンシャルポリシーの作成の詳細については、[クレデンシャルポリシーの作成](#)、(92 ページ) を参照してください。

## クレデンシャルポリシーの作成

クレデンシャルポリシーを作成するには、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Policies] > [Manage Policies] > [Credential Policies] を選択します。
- ステップ 2** [Add] をクリックします。
- ステップ 3** [Add Credential Policy] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Policy Name] フィールド	ポリシーの記述名。
[Description] フィールド	(オプション) ポリシーの説明。
[User Name] フィールド	Cisco IMC ユーザ名またはラックマウントサーバのユーザ名。
[Password] フィールド	Cisco IMC パスワードまたはラックマウントサーバのパスワード。
[Protocol] ドロップダウン リスト	ドロップダウンリストからプロトコルを選択します。
[Port] フィールド	ポリシーのポート番号を入力します。

- ステップ 4** [Submit] をクリックします。
- ステップ 5** 確認ダイアログボックスで、[OK] をクリックします。  
作成したクレデンシャルポリシーのサーバマッピングの編集、複製、削除、表示、適用、確認ができます。

## ハードウェアポリシー

ポリシーは、Cisco IMC でのさまざまな属性設定を定義するための主要なメカニズムです。ポリシーは、複数のサーバにわたって設定の一貫性と反復可能性を確保するうえで役立ちます。包括



的なポリシーセットを定義して使用すると、多数のサーバに類似する設定を適用できるので、一貫性、制御、予測可能性、自動化が促進されます。

**使用例：**自身が管理者である場合、適切なネットワークキング、BIOS、RAID 設定などの必要な設定を含んだ「ゴールデンサーバ」が特定できている場合があります。これらの設定を、ポリシーに準拠していない他のサーバ全体に複製することができます。今後、新しいサーバの追加が必要になる場合や、設定済みサーバを展開する場合に備えて、Cisco IMC内にこの設定を保持することができます。また、同じ内容を適用する前に、その設定をオンザフライで変更することも可能です。たとえば、コンポーネントに更新が必要となったり、NTP IP アドレス、ポーレートなどが必要となる場合があります。「ゴールデンサーバ」での設定を失念していた場合や、他のサーバへの適用前にその内容を確認したい場合もあります。

個々のポリシーは 1 つずつ処理されます。プロファイルにバンドルされているポリシーはマルチスレッド化されており、一連のプロセスを同時に開始するのに役立ちます。

Cisco IMC Supervisor でハードウェアポリシーを使用する方法を次のワークフローに示します。

- 1 BIOS ポリシー、NTP ポリシーなどのハードウェアポリシーを作成します。次のいずれかの方法でポリシーを作成できます。
  - a 新しいポリシーを作成します。さまざまなポリシータイプ、および新しいポリシーの作成方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
  - b サーバ上の既存の設定からポリシーを作成します。サーバ上の既存の設定からポリシーを作成する方法の詳細については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- 2 サーバでポリシーを適用します。ポリシーの適用方法の詳細については、[ハードウェアポリシーの適用](#)、(126 ページ) を参照してください。
- 3 ポリシーで、必要に応じて次のオプション作業を実行します。
  - a Edit
  - b Delete
  - c Clone
  - d また、特定のポリシーにマップされるサーバのリストを表示できます。これらのタスクの実行方法の詳細については、[ハードウェアポリシーでの一般タスク](#)、(127 ページ) を参照してください。
  - e さまざまなポリシーを作成して、それらをプロファイルにグループ化した後、プロファイルをサーバに適用できます。プロファイルの適用方法の詳細については、[ハードウェアプロファイルの適用](#)、(131 ページ) を参照してください。

## ハードウェアポリシーの作成

ハードウェアポリシーを作成するには、次の手順を実行します。

## 手順

- ステップ 1** [Policies] > [Manage Policies and Profiles] を選択します。
- ステップ 2** [Manage Policies and Profiles] ページで、[Hardware Policies] をクリックします。
- ステップ 3** [Add] をクリックします。
- ステップ 4** [Add Policy] ダイアログボックスで、ドロップダウン リストからポリシー タイプを選択します。ポリシータイプに基づくポリシーの作成の詳細については、以下の表に示されているポリシータイプを選んでください。これらのポリシーの設定に必要なさまざまなプロパティは、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』に記載されています。各ポリシー タイプごとに、このマニュアル内の各セクションがリストされています。
- (注) ポリシー作成用の Cisco UCS S3260 プラットフォームを選択するためのチェックボックスが導入されています。このオプションは、デフォルトで無効です。Cisco UCS S3260 のポリシーを作成する必要がある場合、このチェックボックスをオンにして、同様に有効にする必要があります。

ポリシー タイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
BIOS ポリシー, (95 ページ)	BIOS の設定
ディスク グループ ポリシー, (96 ページ)	ストレージ アダプタの管理
FlexFlash ポリシー, (97 ページ)	Flexible Flash コントローラの管理
IPMI Over LAN ポリシー, (101 ページ)	IPMI の設定
LDAP ポリシー, (103 ページ)	LDAP サーバの設定
レガシー ブート順序ポリシー, (104 ページ)	サーバのブート順
ネットワーク構成ポリシー, (105 ページ)	ネットワーク関連の設定
ネットワークセキュリティポリシー, (109 ページ)	ネットワーク セキュリティの設定
NTP ポリシー, (110 ページ)	ネットワーク タイム プロトコル設定の設定
パスワードの有効期限ポリシー, (111 ページ)	パスワードの有効期限切れ
高精度のブート順序ポリシー, (112 ページ)	高精度ブート順の設定
RAID ポリシー, (113 ページ)	ストレージ アダプタの管理
Serial over LAN ポリシー, (115 ページ)	Serial over LAN の設定

ポリシータイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
<a href="#">SNMP ポリシー</a> , (116 ページ)	SNMP の設定
<a href="#">SSH ポリシー</a> , (117 ページ)	SSH の設定
<a href="#">ユーザ ポリシー</a> , (118 ページ)	ローカル ユーザの設定
<a href="#">VIC アダプタ ポリシー</a> , (121 ページ)	VIC アダプタのプロパティの表示
<a href="#">仮想 KVM ポリシー</a> , (120 ページ)	仮想 KVM の設定
<a href="#">vMedia ポリシー</a> , (122 ページ)	仮想メディアの設定
<a href="#">ゾーン分割ポリシー</a> , (123 ページ)	C3260 サーバ向け Cisco UCS C シリーズの統合管理コントローラ GUI の構成ガイド (Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for C3260 Servers) の「Dynamic Storage」

### 次の作業

サーバにポリシーを適用します。ポリシーの適用方法の詳細については、[ハードウェアポリシーの適用](#), (126 ページ) を参照してください。

## BIOS ポリシー

BIOS ポリシーは、サーバの BIOS 設定を自動化します。1つのサーバまたはサーバセットのニーズに適合する特定の BIOS 設定のグループを含む、1つ以上の BIOS ポリシーを作成できます。あるサーバの BIOS ポリシーを指定しない場合、BIOS 設定は一連のデフォルト値 (新品のベアメタルサーバの場合)、または Cisco IMC を使用して設定されている一連の値になります。BIOS ポリシーを指定した場合、ポリシーの値がサーバに設定されている値に置き換わります。

さまざまな BIOS プロパティの設定の詳細については、[Cisco UCS C シリーズサーバの統合管理コントローラ GUI の構成ガイド \(Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide\)](#) の「Configuring BIOS Settings」の項を参照してください。

### 手順

**ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。

このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。

- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [BIOS Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- (注) Cisco IMC Supervisor のプロパティまたは属性のうち、特定の Cisco IMC バージョンを実行するサーバに該当しないものがある場合、それらは適用できません。プロパティが Cisco IMC サーバで利用可能でない場合、そのプロパティフィールドには [Platform-Default] として表示されます。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで、主要な BIOS プロパティ ([Boot Option Retry]、[Post Error Pause]、および [TPM Support] ドロップダウンリストのエントリなど) の値を選択します。
- ステップ 6** [Advanced] ダイアログボックスで、BIOS のプロパティ値をドロップダウン リストから選択して [Next] をクリックします。
- ステップ 7** [Server Management] ダイアログボックスで、サーバのプロパティ値をドロップダウン リストから選択して [Submit] をクリックします。
- ステップ 8** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## ディスク グループ ポリシー

ディスク グループポリシーを使用すると、仮想ドライブに使われる物理ディスクを選択することができ、特定の仮想ドライブに関連するさまざまな属性の設定もできます。仮想ドライブの作成に使用される物理ディスクのグループは、ディスク グループと呼ばれます。

ディスク グループ ポリシーは、ディスク グループの作成方法と設定方法を定義します。このポリシーは、仮想ドライブに使用される RAID レベルを指定します。1つのディスク グループ ポリシーを使用して、複数のディスク グループを管理できます。1つのディスク グループ ポリシーを複数の仮想ドライブに関連付けることができます。その場合、それらの仮想ドライブは同じ仮想ドライブ グループ スペースを共有します。1つの RAID ポリシー内の複数の異なる仮想ドライブに関連付けられるディスク グループポリシーが使用するいずれかの物理ディスクを、別のディスク グループ ポリシーで繰り返し使用することはありません。RAID ポリシーの詳細については、[#unique\\_9](#)を参照してください。

さまざまなディスク グループ プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「*Managing Storage Adapters*」の項を参照してください。

ディスク グループ ポリシーを作成するには、次の手順を実行します。

### 手順

- 
- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウンリストから [Disk Group Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
- ステップ 4** [Virtual Drive Configuration] ダイアログボックスで、RAID レベルを RAID レベルのドロップダウンリストから選択し、[Next] をクリックします。
- ステップ 5** [Local Disk Configuration] ダイアログボックスで、[+] をクリックしてローカルディスク設定を参照するエントリを追加し、[Submit] をクリックします。
- ステップ 6** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- ステップ 7** [Main] ダイアログボックスで [Submit] をクリックします。
- ステップ 8** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- (注)
- サーバの現在の設定からディスクグループポリシーを作成することはできません。
  - サーバの現在の設定から RAID ポリシーが作成されるときに、ディスクグループポリシーもまたサーバ設定から自動的に作成されます。
- 

## FlexFlash ポリシー

FlexFlash ポリシーを使用して、SD カードを設定して有効にすることができます。

さまざまなプロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Managing the Flexible Flash Controller](#)」の項を参照してください。



- (注)
- FlexFlash をサポートする最小の Cisco Integrated Management Controller のファームウェアバージョンは 2.0(2c) です。
  - Flex のフラッシュ ポリシーは、Cisco UCS C3260 ラック サーバでは使用できません。
- 

FlexFlash ポリシーを作成するには、次の手順を実行します。

### 手順

- 
- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。

このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。

**ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [FlexFlash Policy] を選択して [Submit] をクリックします。

**ステップ 3** [Policy Name] フィールドに名前を入力して、[Next] をクリックします。また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。

**ステップ 4** [Configure Cards] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Firmware Mode] ペイン	次のファームウェア動作モードのいずれかを選択します。 <ul style="list-style-type: none"> <li>• [Mirror Mode] : このモードはミラー設定で、C220 M4 および C240 M4 サーバでのみ使用できます。</li> <li>• [Util Mode] : このモードでは、4 つのパーティションを持つ 1 つのカードと、単一パーティションを持つ 1 つのカードが作成されます。このモードを使用できるのは C220 M4 および C240 M4 サーバのみです。</li> <li>• [Not Applicable] : ファームウェアの動作モードが選択されません。[Not Applicable] を選択した場合はステップ 5 に進みます。このモードは、C220 M3、C240 M3、C22、C24、C460 M4 サーバでのみ使用できます。</li> </ul>
[Partition Name] フィールド	パーティションの名前。
[Non Util Card Partition Name] フィールド	2 枚目のカードの単一パーティションに割り当てる名前 (存在する場合)。 (注) このオプションは、util モードの場合にのみ使用できます。
[Select Primary Card] (ミラー モードで使用可能) または [Select Util Card] (Util モードで使用可能) ドロップダウン リスト	SD カードが配置されているスロット [Slot 1] または [Slot 2] を選択するか、または SD カードがサーバに 1 枚しかない場合は [None] を選択します。 (注) [None] は [Select Util Card] オプションでのみ使用できます。

フィールド	説明
[Auto Sync] チェックボックス	<p>選択したスロットで使用可能な SD カードを自動的に同期します。</p> <p>(注) このオプションは、ミラー モードの場合にのみ使用できます。</p>
[Slot-1 Read Error Threshold] フィールド	<p>Cisco FlexFlash カードのスロット 1 へのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p> <p>読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0 (ゼロ) を入力します。</p>
[Slot-1 Write Error Threshold] フィールド	<p>Cisco FlexFlash カードのスロット 1 へのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p> <p>書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0 (ゼロ) を入力します。</p>
[Slot-2 Read Error Threshold] フィールド	<p>Cisco FlexFlash カードのスロット 2 へのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p> <p>読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0 (ゼロ) を入力します。</p> <p>(注) このオプションは、util モードの場合にのみ使用できます。ミラー モードの場合は、スロット 1 の読み取り/書き込みしきい値がスロット 2 にも適用されます。</p>

フィールド	説明
[Slot-2 Write Error Threshold] フィールド	<p>Cisco FlexFlash カードのスロット 2 へのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p> <p>書き込みエラーのしきい値を指定するには、1 ~ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0 (ゼロ) を入力します。</p> <p>(注) このオプションは、util モードの場合にのみ使用できます。ミラーモードの場合は、スロット 1 の読み取り/書き込みしきい値がスロット 2 にも適用されます。</p>

**ステップ 5** ステップ 4 の [Details] ペインで [Not Applicable] を選択した場合は、次のフィールドに値を入力します。

フィールド	説明
[Virtual Drive Enable] ドロップダウン リスト	USB 形式のドライブとして、サーバに対して使用可能にできる仮想ドライブ。
[RAID Primary Member] ドロップダウン リスト	プライマリ RAID メンバが存在するスロット。
[RAID Secondary Role] ドロップダウン リスト	セカンダリ RAID の役割です。
[I/O Read Error Threshold] フィールド	<p>Cisco FlexFlash カードへのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p> <p>読み取りエラーのしきい値を指定するには、1 ~ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0 (ゼロ) を入力します。</p>



フィールド	説明
[I/O Write Error Threshold] フィールド	<p>Cisco FlexFlash カードへのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p> <p>Cisco FlexFlash カードへのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。</p>
[Clear Errors] チェックボックス	オンにした場合、[Submit] をクリックすると、読み取り/書き込みエラーがクリアされます。

**ステップ 6** [Submit] をクリックします。

**ステップ 7** [Submit Result] ダイアログボックスで、[OK] をクリックします。

また、[Hardware Policies] テーブルから既存の FlexFlash ポリシーを選択し、ユーザインターフェイスで該当するオプションを選択することで、適用ステータスの削除、編集、複製、適用、表示が行えます。

(注) FlexFlash ポリシーの適用は、次のように 2 つのステップからなるプロセスです。

- 1 サーバの設定がデフォルトに設定されます。
- 2 ポリシーの新しい設定が適用されます。したがって、この手順で失敗すると、ポリシーを適用する前に既存の設定が失われます。

## IPMI Over LAN ポリシー

インテリジェントプラットフォーム管理インターフェイス (IPMI) では、サーバプラットフォームに組み込まれているサービスプロセッサとのインターフェイスのためのプロトコルを定義しています。このサービスプロセッサはベースボード管理コントローラ (BMC) と呼ばれ、サーバのマザーボードに存在します。BMC は、メインプロセッサおよびボード上の他の要素に、簡単なシリアルバスを使用してリンクします。Cisco IMC を IPMI メッセージで管理するには、IPMI over LAN ポリシーを設定します。

さまざまなプロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring IPMI](#)」の項を参照してください。

IPMI Over LAN ポリシーを作成するには、次の手順を実行します。

## 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [IPMI Over LAN Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力して、[Next] をクリックします。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** ラックマウント サーバ用にこのポリシーを作成している場合は、次の手順を実行します。
- a) [Main] ダイアログボックスで、次のフィールドに値を入力します。

オプション	説明
[Enable IPMI Over LAN]	IPMI プロパティを設定するには、このチェックボックスをオンにします。
[Privilege Level Limit]	ドロップダウン リストから特権レベルを選択します。
[Encryption Key]	このフィールドにキーを入力します。

(注) 暗号キーに含まれる 16 進数文字の数は偶数でなければならない、長さの合計が 40 文字を超えてはなりません。40 文字未満が指定されている場合、キーの長さが 40 になるまでゼロが埋め込まれます。

- b) [Next] をクリックします。
- c) [Confirm] ダイアログボックスで、[Submit] をクリックします。
- d) [Submit Result] ダイアログボックスで、[OK] をクリックします。

[Hardware Policies] ページの [Server Platform] カラムにラックマウントサーバが一覧表示されます。

- ステップ 5 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 6 [CMC Settings] ダイアログボックスで、必要に応じて、CMC 1 と CMC 2 の両方の [Enable IPMI Over LAN] チェックボックスをオンにします。
- ステップ 7 [Next] をクリックします。
- ステップ 8 [BMC Settings] ダイアログボックスで、必要に応じて、BMC 1 と BMC 2 の両方の [Enable IPMI Over LAN] チェックボックスをオンにします。
- ステップ 9 [Confirm] ダイアログボックスで、[Submit] をクリックします。
- ステップ 10 [Submit Result] ダイアログボックスで、[OK] をクリックします。  
[Hardware Policies] ページの [Server Platform] カラムに Cisco UCS C3260 高密度ストレージラックサーバが一覧表示されます。

## LDAP ポリシー

Cisco C シリーズおよび E シリーズ サーバは LDAP をサポートします。Cisco IMC Supervisor は、LDAP ポリシーを使用したサーバでの LDAP 設定をサポートします。1 つのサーバまたはサーバセットのニーズに適合する特定の LDAP 設定のグループを含む、1 つ以上の LDAP ポリシーを作成できます。

さまざまな LDAP プロパティの設定の詳細については、[Cisco UCS C シリーズ サーバの統合管理コントローラ GUI の構成ガイド \(Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide\)](#) の「*Configuring LDAP Server*」の項を参照してください。

### 手順

- ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成 \(93 ページ\)](#) を参照してください。
- ステップ 2 [Add] ダイアログボックスで、ドロップダウンリストから [LDAP Policy] を選択して [Submit] をクリックします。
- ステップ 3 [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成 \(124 ページ\)](#) を参照してください。

- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで、LDAP プロパティを入力します。
- ステップ 6** [Next] をクリックします。
- ステップ 7** [LDAP Servers] ダイアログボックスで、LDAP サーバの詳細を入力します。
- ステップ 8** [Next] をクリックします。
- ステップ 9** [Group Authorization] ダイアログボックスでグループ認証の詳細を入力し、[+] をクリックして LDAP グループ エントリをテーブルに追加します。
- ステップ 10** [Add Entry to LDAP Groups] ダイアログボックスで、グループの詳細を入力します。
- ステップ 11** [Submit] をクリックします。
- ステップ 12** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- ステップ 13** [Group Authorization] ダイアログボックスで [Submit] をクリックします。
- ステップ 14** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- (注)
- サーバに設定されている既存の LDAP ロールグループはすべて削除され、ポリシーで設定したロールグループに置き換えられます。ポリシーにロールグループを追加していない場合、サーバ上の既存のロールグループは単純に削除されます。
  - [Nested Group Search Depth] は、Cisco IMC バージョン 2.0(4c) 以上にのみ適用できます。2.0(4c) より前のバージョンの Cisco IMC を実行しているサーバには、ポリシーを使ってこの値を適用することはできません。

## レガシー ブート順序ポリシー

レガシー ブート順序ポリシーは、ブート順序の設定を自動化します。1つのサーバまたはサーバセットのニーズに適合する特定のブート順序設定のグループを含む、1つ以上のレガシー ブート順序ポリシーを作成することができます。Cisco IMC Supervisor を使用して、使用可能なブートデバイス タイプからサーバがブートを試行する順序を設定できます。また、デバイスの線形順序付けを可能にする高精度ブート順序を設定することもできます。高精度ブート順序の詳細については、[#unique\\_132](#)を参照してください。

さまざまなサーバブート順序プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「*Server Boot Order*」の項を参照してください。



(注) 従来のブート順序ポリシーは、Cisco UCS C3260ラック サーバでは使用できません。

### 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。

このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。

- ステップ 2** [Add] ダイアログボックスで、ドロップダウンリストから [Legacy Boot Order Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力して、[Next] をクリックします。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** [Main] ダイアログボックスで [+] をクリックして、ドロップダウンリストからデバイス タイプを選択します。追加したデバイスがテーブルにリストされます。  
[Select Devices] テーブルで、既存のデバイスを選択して [x] をクリックするとデバイスが削除されます。エントリの順序を変更するには、上/下矢印アイコンを使用します。テーブルのエントリの順序により、ブート順序が決まります。  
  
同じデバイス タイプをさらに追加することはできません。
- ステップ 5** [Add Entry to Select Devices] ダイアログボックスで [Submit] をクリックします。
- ステップ 6** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- ステップ 7** [Main] ダイアログボックスで [Submit] をクリックします。
- ステップ 8** [Submit Result] ダイアログボックスで、[OK] をクリックします。  
(注) このポリシーは、2.0 より前のバージョンの Cisco IMC にのみ適用できます。それ以降のバージョンの Cisco IMC を実行するサーバに対してポリシーが適用された場合、エラーメッセージが表示されます。代わりに高精度ブート順序ポリシーを使用してください。

## ネットワーク構成ポリシー

Cisco IMC Supervisor では、サーバの以下のネットワーク設定を指定できるネットワーク構成ポリシーを作成できます。

- DNS ドメイン
- IPv4 および IPv6 用の DNS サーバ
- VLAN コンフィギュレーション

さまざまなネットワーク構成プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring Network-Related Settings](#)」の項を参照してください。

ネットワーク構成ポリシーを作成するには、次の手順を実行します。

## 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [Network Configuration Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力して、[Next] をクリックします。また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** ラックマウント サーバ用にこのポリシーを作成している場合は、次の手順を実行します。
- a) [Main] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Common Properties]	
[Use Dynamic DNS] チェックボックス	ダイナミック DNS は、Cisco IMC Supervisor から DNS サーバのリソース レコードを追加または更新するために使用されます。
[Use Dynamic DNS] チェックボックスをオンにした場合	
[Dynamic DNS Update Domain] フィールド	ドメインを指定できます。ドメインは、メインドメインまたはサブドメインのどちらでも可です。このドメイン名は、DDNS 更新のために Cisco IMC Supervisor のホスト名に付加されます。
[IPv4 Properties]	
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバアドレスを DHCP から取得します。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
[IPv6 Properties]	
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバアドレスを DHCP から取得します。

フィールド	説明
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
[VLAN Properties]	
[Enable VLAN] チェックボックス	オンにすると、仮想 LAN に接続されます。
[Enable VLAN] チェックボックスをオンにした場合	
[VLAN ID] フィールド	VLAN ID。
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

- b) [Next] をクリックします。
- c) [Confirm] ダイアログボックスで、[Submit] をクリックします。
- d) [Submit Result] ダイアログボックスで、[OK] をクリックします。  
 [Hardware Policies] ページの [Server Platform] カラムにラックマウントサーバが一覧表示されます。

**ステップ 5** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。

**ステップ 6** [Main] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Common Properties]	
[Use Dynamic DNS] チェックボックス	ダイナミック DNS は、Cisco IMC Supervisor から DNS サーバのリソース レコードを追加または更新するために使用されます。
[Use Dynamic DNS] チェックボックスをオンにした場合	
[Dynamic DNS Update Domain] フィールド	ドメインを指定できます。ドメインは、メインドメインまたはサブドメインのどちらでも可です。このドメイン名は、DDNS 更新のために Cisco IMC Supervisor のホスト名に付加されます。
[IPv4 Properties]	

フィールド	説明
[Use DHCP] チェックボックス	オンにすると、[Obtain DNS Server Addresses from DHCP] チェックボックスが表示されます。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、DNS の DHCP が有効になります。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
[IPv6 Properties]	
[Enable IPv6] チェックボックス	オンにすると、[Use DHCP] チェックボックスが表示されます。
[Use DHCP] チェックボックス	オンにすると、[Obtain DNS Server Addresses from DHCP] チェックボックスが表示されます。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバアドレスを DHCP から取得します。
[Use DHCP] チェックボックスをオフにした場合	
[Management IP Address] フィールド	管理 IP アドレスを入力します。
[Prefix Length] フィールド	プレフィックス長の文字数を入力します。
[Gateway] フィールド	ゲートウェイの IP アドレスを入力します。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
[VLAN Properties]	
[Enable VLAN] チェックボックス	オンにすると、仮想 LAN に接続されます。
[Enable VLAN] チェックボックスをオンにした場合	
[VLAN ID] フィールド	VLAN ID。



フィールド	説明
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

**ステップ 7** [Next] をクリックします。

**ステップ 8** [CMC Settings] ダイアログボックスで、必要に応じて、CMC 1 と CMC 2 の両方の以下のフィールドに入力します。

フィールド	説明
[Hostname] フィールド	サーバのホスト名。
[IPv4 Address] フィールド	IPv4 の IP アドレス。
[IPv6 Address] フィールド	IPv6 の IP アドレス。

**ステップ 9** [Next] をクリックします。

**ステップ 10** [BMC Settings] ダイアログボックスで、必要に応じて、BMC 1 と BMC 2 の両方の以下のフィールドに入力します。

フィールド	説明
[Hostname] フィールド	サーバのホスト名。
[IPv4 Address] フィールド	IPv4 の IP アドレス。
[IPv6 Address] フィールド	IPv6 の IP アドレス。

**ステップ 11** [Next] をクリックします。

**ステップ 12** [Confirm] ダイアログボックスで、[Submit] をクリックします。

**ステップ 13** [Submit Result] ダイアログボックスで、[OK] をクリックします。

**注意** ネットワークの DHCP の設定によって決まる Cisco IMC Supervisor とラックサーバ間の通信の中断を防ぐために、以下の設定を使用する際には注意してください。

DNS IP アドレスを取得するために DHCP を使用している場合、サーバの管理 IP アドレスに DHCP を使用するために（このポリシーが適用される）ラックサーバも設定されます。

## ネットワークセキュリティポリシー

Cisco IMC Supervisor は、ネットワークセキュリティとして IP ブロッキングを使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接

続を防ぎます。IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバ、またはその他のインターネット サーバへの不要な接続を効果的に禁止します。1 つのサーバまたはサーバセットのニーズに適合する特定の IP プロパティのグループを含む、1 つ以上のネットワークセキュリティ ポリシーを作成できます。

さまざまなネットワークセキュリティプロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Network Security Configuration](#)」の項を参照してください。

ネットワークセキュリティポリシーを作成するには、次の手順を実行します。

## 手順

- 
- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [Network Security] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [IP Blocking] ダイアログボックスで、IP をブロックするために [Enable IP Blocking] チェックボックスをオンにし、IP ブロック プロパティを設定するための属性を入力して、[Next] をクリックします。
- ステップ 6** [IP Filtering] ダイアログボックスで、[Enable IP Filtering] チェックボックスをオンにして IP を有効にし、単一の IP アドレスまたは IP アドレスの範囲を入力します。  
(注) フィルタ 1 はデフォルトで Cisco IMC Supervisor の IP アドレスを表示します。
- ステップ 7** [Submit] をクリックします。
- ステップ 8** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## NTP ポリシー

NTP サービスを使用すると、NTP サーバとの間で時刻を同期するよう、Cisco IMC Supervisor によって管理されるサーバを設定できます。デフォルトでは、Cisco IMC Supervisor では NTP サーバが動作しません。NTP サービスを有効にして設定する必要があります。その際、NTP サーバとして動作する少なくとも 1 台、最大 4 台のサーバの IP/DNS アドレスを指定します。NTP サービス

を有効にすると、Cisco IMC Supervisor は、管理対象サーバと設定済み NTP サーバとの間で時刻を同期します。

さまざまな NTP プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring Network Time Protocol Settings](#)」の項を参照してください。

NTP ポリシーを作成するには、次の手順を実行します。

#### 手順

- 
- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [NTP Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで、[Enable NTP] チェックボックスをオンにして代替サーバを有効にし、NTP サーバを 4 つまで指定します。
- ステップ 6** [Submit] をクリックします。
- ステップ 7** [Submit Result] ダイアログボックスで、[OK] をクリックします。  
(注) このポリシーは、E シリーズ サーバ モデルには適用できません。
- 

## パスワードの有効期限ポリシー

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。ユーザは、ユーザポリシーの一部として構成を設定して派生させ、パスワード有効期限ポリシーを作成することができます。

さまざまなプロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring Password Expiry for Users](#)」の項を参照してください。

パスワード有効期限ポリシーを作成するには、次の手順を実行します。

## 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [Password Expiration Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。
- ステップ 4** [Main] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Enable Password Expiry] チェックボックス	指定したパスワードの有効期限を有効にするには、このチェックボックスをオンにして、次の項目を入力します。  [Password Expiry Duration] : パスワードが期限切れになる日数を設定します。
[Password History] フィールド	パスワード履歴を表示するときに表示される発生数を設定します。
[Notification Period] フィールド	パスワードの有効期限について通知されるまでの日数を設定します。
[Grace Period] フィールド	パスワードの期限が切れるまでの猶予期間を設定します。

- ステップ 5** [Submit] をクリックします。
- (注)
- 既存のポリシーを選択し、[Properties] または [Delete] をクリックして、[More Actions] ドロップダウンリストからポリシーを編集または削除することもできます。
  - このポリシーは、ユーザポリシーとともに適用する必要があります。パスワード有効期限ポリシーを個別に適用することはできません。
  - E シリーズ サーバは、パスワード有効期限ポリシーをサポートしていません。

## 高精度のブート順序ポリシー

高精度のブート順序を設定すると、デバイスの線形順序付けが可能になります。Cisco IMC Supervisor では、ブート順序とブートモードの変更、各デバイス タイプの下への複数のデバイスの追加、ブート順序の並び替え、各デバイス タイプのパラメータの設定ができます。

さまざまなブート順序プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「*Configuring the Precision Boot Order*」の項を参照してください。

このポリシーは、Cisco IMC バージョン 2.x 以上を実行しているサーバ用に作成できます。2.x より前のバージョンを実行しているサーバの場合、代わりにレガシーブート順序ポリシーを設定する必要があります。

高精度ブート順序ポリシーを作成するには、次の手順を実行します。

## 手順

- 
- ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
  - ステップ 2 [Add] ダイアログボックスで、ドロップダウンリストから [Precision Boot Order Policy] を選択して [Submit] をクリックします。
  - ステップ 3 [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
  - ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
  - ステップ 5 [Main] ダイアログボックスで、[UEFI Secure Boot] チェックボックスをオンにするか、[Configure Boot Mode] ドロップダウンリストからブートモードを選択します。
  - ステップ 6 [+] をクリックして、デバイスの詳細を選択または入力します。追加したデバイスがテーブルにリストされます。  
また、[Select Devices] テーブルで既存のデバイスを選択し、[x] をクリックして削除したり、編集アイコンをクリックしてデバイスを編集したりすることもできます。エントリの順序を変更するには、上/下矢印アイコンを使用します。テーブルのエントリの順序により、ブート順序が決まります。
  - ステップ 7 [Add Entry to Select Devices] ダイアログボックスで [Submit] をクリックします。
  - ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。
  - ステップ 9 [Main] ダイアログボックスで [Submit] をクリックします。
  - ステップ 10 [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## RAID ポリシー

RAID ポリシーを使用すると、サーバ上に仮想ドライブを作成できます。仮想ドライブのストレージ容量も設定できます。RAID ポリシー内のそれぞれの仮想ドライブは、1つのディスクグループ

ポリシーに関連付けられます。ディスクグループポリシーを使用すると、特定の仮想ドライブに使われるディスクを選択し、設定することができます。

RAID ポリシーは、以下の環境でのみサポートされます。

- RAID 設定をサポートするストレージコントローラ。
- Cisco IMC ファームウェア バージョン 2.0(4c) 以上。
- 単一のストレージコントローラを含むサーバ。複数のストレージコントローラを含むサーバでは、RAID ポリシーは最初のスロットのストレージコントローラにのみ適用されます。

さまざまなプロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Managing Storage Adapters](#)」の項を参照してください。

RAID ポリシーを作成するには、次の手順を実行します。

## 手順

- 
- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウンリストから [RAID Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで [+] をクリックして、サーバ上に設定する仮想ドライブを追加します。
- ステップ 6** [Add Entry to Virtual Drives] ダイアログボックスで、仮想ドライブの詳細 ([Virtual Drive Name] や [Virtual Drive Size] など) を入力します。
- ステップ 7** [Disk Group Policy] ドロップダウンリストから既存のディスクグループポリシーを選択するか、または [+] をクリックし、新しいディスクグループポリシーを追加してローカルディスクを指定します。ディスクグループポリシーを作成するには、[#unique\\_133](#)を参照してください。  
(注) 2つの仮想ドライブが作成されて同じディスクグループポリシーに関連付けられた場合、それらは同じ仮想ドライブグループスペースを共有します。

- ステップ 8** [Access Policy]、[Read Policy]、[Write Policy]、[IO Policy]、および [Drive Cache] ドロップダウンリストに表示されているオプションから選択します。
- ステップ 9** [Expand to available] チェックボックスをオンにして、ディスクで使用可能な最大容量を使用するために、仮想ドライブのサイズを拡張します。
- ステップ 10** [Boot Drive] チェックボックスをオンにして、作成している仮想ドライブをブートドライブとして設定します。  
(注) 複数のブートドライブを設定することはできません。
- ステップ 11** [Set disks in JBOD state to Unconfigured Good] チェックボックスをオンにして、JBOD 状態にあるディスクを、それらが仮想ドライブの作成に使用される前に Unconfigured Good 状態に設定します。
- ステップ 12** [Add Entry] ダイアログボックスで [Submit] をクリックします。
- ステップ 13** [Submit Result] ダイアログボックスで、[OK] をクリックします。  
作成した仮想ドライブは [Virtual Drives] テーブルで確認できます。
- ステップ 14** [Delete existing Virtual Drives] チェックボックスをオンにして、サーバ上の既存のすべての仮想ドライブを削除します。  
このチェックボックスを選択した場合、ポリシーの適用時に、サーバ上の既存のすべての仮想ドライブが削除されます。この結果、既存のデータが失われることがあります。
- ステップ 15** [Configure Unused Disks] チェックボックスをオンにし、未使用ディスクを [Unconfigured Good] または [JBOD] 状態に設定するオプションを選択します。
- ステップ 16** [Main] ダイアログボックスで [Submit] をクリックします。
- ステップ 17** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## Serial over LAN ポリシー

Serial over LAN を使用すると、管理対象システムのシリアルポートの入出力を IP 経由でリダイレクトできます。Cisco IMC Supervisor を使用してホスト コンソールに到達するには、サーバで Serial over LAN を設定して使用します。1 つのサーバまたはサーバセットのニーズに適合する特定の Serial over LAN 属性のグループを含む、1 つ以上の Serial over LAN ポリシーを作成できます。

さまざまな Serial over LAN プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring Serial Over LAN](#)」の項を参照してください。

Serial over LAN ポリシーを作成するには、次の手順を実行します。

### 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。



- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [Serial Over LAN Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されません。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、[\(124 ページ\)](#) を参照してください。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで、[Enable SoL] チェックボックスをオンにして、ドロップダウン リストから [CoM Port] 値と [Baud Rate] 値を選択するか、既存の値を使用します。
- ステップ 6** [Submit] をクリックします。
- ステップ 7** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## SNMP ポリシー

Cisco IMC Supervisor は Simple Network Management Protocol (SNMP) の設定をサポートし、管理対象サーバから SNMP トラップによって障害とアラートの情報を送信するための設定が可能です。

さまざまな SNMP プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring SNMP](#)」の項を参照してください。

SNMP ポリシーを作成するには、次の手順を実行します。

### 手順

---

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、[\(93 ページ\)](#) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [SNMP Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されません。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、[\(124 ページ\)](#) を参照してください。



- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [SNMP Users] ダイアログボックスで [+] をクリックして SNMP ユーザを追加し、ユーザの詳細情報を入力します。[+] アイコンを使用して、最大で 15 SNMP ユーザを追加することができます。既存の SNMP エントリを選択すると、そのエントリを編集またはテーブルから削除できます。
- ステップ 6** [Next] をクリックします。
- ステップ 7** [SNMP Traps] ダイアログボックスで [+] をクリックして SNMP トラップを追加し、トラップの詳細情報を入力します。[+] アイコンを使用して、最大で 15 個の SNMP トラップを追加することができます。既存の SNMP エントリを選択すると、そのエントリを編集またはテーブルから削除できます。
- ステップ 8** [Next] をクリックします。
- ステップ 9** [SNMP Settings] ダイアログボックスで、SNMP プロパティを設定します。
- ステップ 10** [Submit] をクリックします。
- ステップ 11** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- (注)
- サーバで以前に設定されていた既存の [SNMP Users] または [SNMP Traps] が削除され、ポリシーで設定したユーザやトラップに置き換わります。ポリシーにユーザやトラップをまだ追加していない場合は、サーバ上の既存のユーザまたはトラップが削除されますが、置き換わりません。
  - 2.x より前のバージョンの Cisco IMC を実行している C シリーズサーバでは [SNMP Port] を設定できません。チェックボックスを使用して、そのようなサーバは除外する必要があります。
  - Cisco IMC バージョン 2.x を実行している E シリーズサーバでは [SNMP Port] を設定できません。チェックボックスを使用して、そのようなサーバは除外する必要があります。

## SSH ポリシー

SSH サーバは、SSH クライアントがセキュアな暗号化された接続を行えるようにします。SSH クライアントは、SSH プロトコルで動作し、デバイスの認証および暗号化を提供するアプリケーションです。1 つのサーバまたはサーバセットのニーズに適合する特定の SSH プロパティのグループを含む、1 つ以上の SSH ポリシーを作成することができます。

さまざまな SSH プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring SSH](#)」の項を参照してください。

SSH ポリシーを作成するには、次の手順を実行します。

### 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。

このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。

- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [SSH Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されません。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで [Enable SSH] チェックボックスをオンにして、SSH プロパティを入力するか、または既存のプロパティを使用します。
- ステップ 6** [Submit] をクリックします。
- ステップ 7** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## ユーザポリシー

ユーザポリシーは、ローカルユーザの設定を自動化します。1つのサーバまたはサーバのグループに設定される必要のあるローカルユーザリストを含む、1つ以上のユーザポリシーを作成することができます。

さまざまなプロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring Local Users](#)」の項を参照してください。

ユーザポリシーを作成するには、次の手順を実行します。

### 手順

---

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウン リストから [User Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されません。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。

- ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5 [Main] ダイアログボックスで、サーバに設定する必要があるユーザを [Users] リストに追加できます。
- ステップ 6 次のステップで設定するユーザに強力なパスワードを適用する場合は、[Enforce Strong Password] チェックボックスをオンにします。  
この機能は、CIMC 2.0(9c) 以上を実行しているサーバにのみ適用できます。
- ステップ 7 [+] をクリックして、ユーザを追加します。
- ステップ 8 [Add Entry to Users] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
[Username]	ユーザの名前をフィールドに入力します。
[Role]	読み取り専用、管理などのユーザ ロールをドロップダウン リストから選択します。
[Enable User Account]	ユーザをアクティブにするには、このチェックボックスをオンにします。
[New Password]	ユーザ名に関連付けられるパスワードを入力します。
[Confirm New Password]	前のフィールドと同じパスワードを入力します。

- ステップ 9 [Submit] をクリックします。
- ステップ 10 パスワード有効期限ポリシーを適用するには、[Add Password Expiration Policy] チェックボックスをオンにします。  
(注) パスワード有効期限ポリシーを個別に適用することはできません。
- ステップ 11 既存のパスワード有効期限ポリシーをドロップダウンリストから選択するか、または[+]をクリックして新しいパスワード有効期限ポリシーを追加します。新しいパスワード有効期限ポリシーの作成方法の詳細については、[パスワードの有効期限ポリシー](#)、(111 ページ) を参照してください。
- ステップ 12 [Submit] をクリックします。  
また、[Main] ダイアログボックスの [Users] テーブルで既存のユーザを選択し、[Edit] または [Delete] アイコンをクリックしてユーザを編集/削除することもできます。

- (注)
- [Users] テーブルの最初のユーザは、管理ユーザです。この管理ユーザを削除することはできませんが、パスワードは変更できます。
  - 2.0(8d) より古いバージョンの CIMC を実行しているサーバの場合、Cisco IMC Supervisor により、ポリシーで定義されているものとともに、サーバにダミーのユーザエントリが作成されています。CIMC 2.0(8d) 以上を実行しているサーバにポリシーを適用する場合、ブランク ユーザエントリは作成されません。（以前のポリシーにより適用された）既存のダミーユーザエントリはクリアされます。
  - Cisco IMC Supervisor を管理するためのアカウントがポリシーのユーザリストから削除されていないことを確認します。削除した場合、Cisco IMC Supervisor は管理対象サーバへの接続を失います。

## 仮想 KVM ポリシー

KVM コンソールは Cisco IMC Supervisor からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス (KVM) の直接接続をエミュレートします。KVM コンソールを使用すると、リモートの場所からサーバに接続できます。1つのサーバまたはサーバセットのニーズに適合する特定の仮想 KVM プロパティのグループを含む、1つ以上の KVM ポリシーを作成することができます。

さまざまな KVM プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring the Virtual KVM](#)」の項を参照してください。

仮想 KVM ポリシーを作成するには、次の手順を実行します。

### 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウンリストから [Virtual KVM Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。

- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Enable vKVM] チェックボックスをオンにします。
- ステップ 6** 仮想サーバ プロパティを選択または入力するか、既存のプロパティを使用します。
- ステップ 7** [Submit] をクリックします。
- ステップ 8** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## VIC アダプタ ポリシー

さまざまな VIC アダプタ プロパティの設定の詳細については、[Cisco UCS C シリーズ サーバの統合管理コントローラ GUI の構成ガイド \(Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide\)](#) の「*Viewing VIC Adapter Properties*」の項を参照してください。

### 手順

---

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成, \(93 ページ\)](#) を参照してください。
- ステップ 2** [Add] ダイアログボックスで、ドロップダウンリストから [VIC Adapter Policy] を選択して [Submit] をクリックします。
- ステップ 3** [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成, \(124 ページ\)](#) を参照してください。
- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで [+] をクリックして、VIC アダプタ エントリをテーブルに追加します。
- ステップ 6** [Add Entry to VIC Adapters] ダイアログボックスで、アダプタの詳細を入力または選択します。
- [vNIC] : デフォルト プロパティは eth0 および eth1 です。これらのプロパティは編集のみが可能であり、削除はできません。また、usNIC プロパティでもこれらのプロパティを使用できます。
  - [vHBA] : デフォルト プロパティは fc0 および fc1 です。これらのプロパティは編集のみが可能であり、削除はできません。

- ステップ7 [Submit] をクリックします。
- ステップ8 [Submit Result] ダイアログボックスで、[OK] をクリックします。
- ステップ9 [Main] ダイアログボックスで [Submit] をクリックします。
- ステップ10 [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## vMedia ポリシー

KVM コンソールおよび vMedia を使ってサーバに OS をインストールするために、Cisco IMC Supervisor を使用できます。1つのサーバまたはサーバセットのニーズに適合する、さまざまな OS イメージ用の vMedia マッピングを含む1つ以上の vMedia ポリシーを作成することができます。Cisco IMC Supervisor では、最大で2つの vMedia マッピングを設定できます。1つは (CDD を介した) ISO ファイル用、もう1つは (HDD を介した) IMG ファイル用です。

さまざまな vMedia プロパティの設定の詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide](#)』の「[Configuring Virtual Media](#)」の項を参照してください。

vMedia ポリシーを作成するには、次の手順を実行します。

### 手順

---

- ステップ1 [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ2 [Add] ダイアログボックスで、ドロップダウン リストから [vMedia Policy] を選択して [Submit] をクリックします。
- ステップ3 [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。

- ステップ 4** Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
- ステップ 5** [Main] ダイアログボックスで、[Enable vMedia] チェックボックスをオンにして vMedia を有効にし、[Enable Virtual Media Encryption] をオンにして vMedia 暗号化を有効にします。
- ステップ 6** [Next] をクリックします。
- ステップ 7** [Add CDD vMedia Mapping] チェックボックスをオンにして、CDD マッピングの詳細を入力します。
- ステップ 8** [Next] をクリックします。
- ステップ 9** [Add HDD vMedia Mapping] チェックボックスをオンにして、HDD マッピングの詳細を入力します。
- ステップ 10** [Submit] をクリックします。
- ステップ 11** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- (注)
- 現在、Cisco IMC Supervisor では [Low Power USB State] を設定できません。
  - vMedia ポリシーを適用すると、ポリシーに vMedia マッピングが含まれない場合でも、それまでサーバに設定されていた既存の vMedia マッピングがすべて削除されます。

## ゾーン分割ポリシー

ゾーン分割ポリシーは、サーバに物理ドライブを割り当てるために使用されます。Cisco UCS C3260 高密度ストレージラックサーバは、Cisco Management Controller (CMC) の Serial Attached SCSI (SAS) ドライブのダイナミックストレージをサポートしています。このダイナミックストレージのサポートは、CMC の SAS Fabric Manager によって提供されます。ダイナミックストレージは次のオプションをサポートしています。

- サーバ 1 およびサーバ 2 への物理ディスクの割り当て
- シャーシ幅ホットスペア (RAID コントローラでのみサポート)
- 共有モード (HBA でのみサポート)
- 物理ディスクの割り当て解除
- SAS エクスパンダプロパティの表示
- サーバへの物理ドライブの割り当て
- シャーシ幅ホットスペアとしての物理ドライブの移動
- 物理ドライブの割り当て解除

さまざまなディスクグループプロパティの設定の詳細については、[C3260 サーバ向け Cisco UCS C シリーズの統合管理コントローラ GUI の構成ガイド \(Cisco UCS C-Series Integrated Management](#)



[Controller GUI Configuration Guide for C3260 Servers](#) の「*Dynamic Storage*」の項を参照してください。

ゾーン分割ポリシーを作成するには、次の手順を実行します。

### 手順

- 
- ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
  - ステップ 2 [Add] ダイアログボックスで、ドロップダウンリストから [Zoning Policy] を選択して [Submit] をクリックします。
  - ステップ 3 [Policy Name] フィールドに名前を入力します。  
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、[既存の設定からのポリシーの作成](#)、(124 ページ) を参照してください。  

(注) ゾーン分割ポリシーは、Cisco UCS 3260 ラック サーバにのみ適用可能なため、UI の [Cisco UCS C3260] チェック ボックスはデフォルトでオンになっています。
  - ステップ 4 [Zoning] ダイアログボックスで [+] をクリックして、サーバ上に設定するローカルディスクを追加します。
  - ステップ 5 [Add Entry to Local Disks] ダイアログボックスで、ローカルディスクが存在する [Slot Number] を入力します。
  - ステップ 6 ローカルディスクの詳細（ローカルディスクの所有権を割り当てる [Ownership] など）を選択します。
  - ステップ 7 あるサーバが所有するディスクを別のサーバに割り当てる場合は、[Force] チェックボックスをオンにします。
  - ステップ 8 [Submit] をクリックします。
  - ステップ 9 [Submit Result] ダイアログボックスで、[OK] をクリックします。
  - ステップ 10 ポリシーを設定するには、[Modify Physical Drive Power Policy] チェックボックスをオンにします。
  - ステップ 11 [Physical Drive Power State] ドロップダウンリストから電源の状態を選択します。
  - ステップ 12 [Submit] をクリックします。
  - ステップ 13 [Submit Result] ダイアログボックスで、[OK] をクリックします。
- 

## 既存の設定からのポリシーの作成

すでに設定済みのサーバを使用してポリシーを作成することもできます。サーバ上の既存の設定を再使用すると、類似する設定を作成するのに必要な時間と労力を軽減できます。





(注) サーバの現在の設定からポリシーを作成するときには、サーバからパスワードフィールドが取得されません。

サーバの現在の設定からポリシーを作成するには、次の手順を実行します。

#### 手順

- ステップ 1** [Hardware Policies] ページで、[Add] をクリックします。  
このページに移動する方法の詳細については、[ハードウェアポリシーの作成](#)、(93 ページ) を参照してください。
- ステップ 2** [Create policy from current configuration of the server] チェックボックスをオンにして、[Next] をクリックします。
- ステップ 3** [Server Details] ダイアログボックスで、[Create policy from current configuration of the server] チェックボックスをオンにします。次の2つの方法でサーバの詳細情報を使用できます。Cisco UCS C3260 サーバの場合はステップ 5 に進みます。
- [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。
    - [Server IP] フィールドに IP アドレスを入力します。
    - 既存のポリシーを選択するために [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[Credential Policy Add Form] ダイアログボックスで詳細を入力して新規ポリシーを作成します。
    - [User Name] フィールドにサーバ ログイン名を入力します。
    - [Password] フィールドにサーバ ログイン パスワードを入力します。
    - [Protocol] ドロップダウン リストから http または https を選択します。
    - [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。
  - [Select] をクリックして、設定の取得元となるサーバを選択します。
- ステップ 4** [Next] をクリックします。  
[Main] ダイアログボックスに進みます。ポリシーの作成を続けます。
- ステップ 5** Cisco UCS C3260 サーバの場合は、[Create policy from current configuration of the server] および [Cisco UCS C3260] チェックボックスの両方をオンにして、[Next] をクリックします。
- ステップ 6** [Server Details] ダイアログボックスで [Enter Server Details Manually] チェックボックスをオンにして、以下のフィールドに入力するか、または [Select] をクリックして、ポリシーを適用する Cisco UCS C3260 サーバを選択します。
- Cisco UCS C3260 プラットフォームの [Server IP] フィールドに仮想的な管理 IP アドレスを入力します。

- 2 既存のポリシーを選択するために [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウンリストからポリシーを選択するか、[Credential Policy] ドロップダウンリストの横にある [+] をクリックし、[Credential Policy Add Form] ダイアログボックスで詳細を入力して新規ポリシーを作成します。
- 3 [User Name] フィールドにサーバログイン名を入力します。
- 4 [Password] フィールドにサーバログインパスワードを入力します。
- 5 [Protocol] ドロップダウンリストから http または https を選択します。
- 6 [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。

ステップ 7 [Server Node 1] または [Server Node 2] のオプション ボタンを選択します。

ステップ 8 [Next] をクリックします。  
[Main] ダイアログボックスに進みます。ポリシーの作成を続けます。

## ハードウェアポリシーの適用

既存のポリシーをサーバに適用するには、次の手順を実行します。

### 手順

- ステップ 1 メニュー バーで、[Policies] > [Manage Policies] を選択します。
- ステップ 2 [Hardware Policies] タブを選択します。
- ステップ 3 左側のペインから、適用するポリシーを選択します。
- ステップ 4 上部にある利用可能なオプションから、[Apply] をクリックします。  
[Apply Policy] ダイアログボックスで、ポリシーを適用する [Chassis] または [Server(s)] を選択できます。これらのオプションは、選択したユーザ管理ポリシーまたはコンピューティングノードポリシーに基づいて表示されます。
- ステップ 5 [Select] をクリックして、ポリシーを適用するシャーシまたはサーバを選択します。  
(注) Cisco UCS 3260 タイプのポリシーの場合、シャーシは管理ポリシーとして、サーバはコンピューティングノードポリシーとして表示されます。管理ポリシーとコンピューティングノードポリシーの詳細については、[ポリシーとプロファイル](#)、(158 ページ) を参照してください。
- ステップ 6 ポリシー タスクの適用を後でスケジュールするには、[Schedule Later] チェックボックスをオンにします。
- ステップ 7 [Schedule] ドロップダウンリストから既存のスケジュールを選択するか、[+] をクリックして新しいスケジュールを作成します。スケジュール作成の詳細については、[スケジュールの作成](#)、(143 ページ) を参照してください。

(注) [Policies]>[Manage Schedules]の順に移動して、スケジュールを選択し、[View Scheduled Tasks]をクリックしてスケジュールされたタスクを表示するか、または[Remove Scheduled Tasks]をクリックしてスケジュールされたタスクを削除できます。

**ステップ 8** [Submit] をクリックします。

**ステップ 9** [Submit Result] ダイアログボックスで、[OK] をクリックします。  
指定したサーバセットにポリシーを適用するプロセスが開始します。ポリシーの種類、およびポリシーが適用されるサーバへのネットワーク接続に応じて、このプロセスに数分かかる場合があります。

## ハードウェア ポリシーでの一般タスク

既存のポリシーのサーバマッピング詳細を編集、削除、複製、または表示するには、次の手順を実行します。

### 手順

**ステップ 1** メニューバーで、[Policies]>[Manage Policies and Profiles] を選択します。

**ステップ 2** [Hardware Policies] タブを選択します。

**ステップ 3** [Hardware Policies] ページで、左側ペインのポリシーを展開して、ポリシーを選択します。オプションで次の手順を実行することができます。

- a) (任意) ポリシーを削除するには、[Delete] をクリックします。[Delete Policy] ダイアログボックスで[Select] をクリックし、削除するポリシーを選択します。[Select] および [Submit] をクリックします。  
ポリシーがサーバに関連付けられていても、選択した1つ以上のポリシーを削除できます。プロフィールに関連付けられたポリシーを削除しようとすると、エラーになります。
- b) (任意) ポリシーを変更するには、[Properties] をクリックし、必要に応じてプロパティを変更します。  
ポリシー名を変更するときには、すでに存在する名前を指定しないでください。
- c) (任意) ポリシーを複製するには、[Clone] をクリックして、選択したポリシーの詳細を新しいポリシーにコピーします。
- d) (任意) [View Details] をクリックすると、すでに適用したポリシーのステータス、およびポリシーが適用されたサーバIPアドレスが表示されます。ポリシーが正常に適用されない場合、[Status Message] 列にエラーメッセージが表示されます。

**ステップ 4** サーバまたはサーバグループにポリシーを適用するには、[Apply] をクリックします。プロフィールを適用する方法の詳細については、[ハードウェアポリシーの適用](#)、(126 ページ) を参照してください。

**ステップ 5** 状況に応じて [Submit] または [Close] をクリックします。

## ハードウェア プロファイル

複数のポリシーを組み合わせて、ハードウェア プロファイルが形成されます。たとえば、1つのラック ハードウェア プロファイル設定の詳細情報を複数のラックマウント サーバに適用することができます。いくつかの特定のラックマウントサーバにこのハードウェアプロファイルを関連付けることができます。これにより、複数のサーバにわたって設定の一貫性と反復可能性が確保されます。プロファイルを定義して使用すると、類似する設定が多数のサーバに適用されるため、一貫性、制御、予測可能性、自動化が促進されます。

次のワークフローは、Cisco IMC Supervisor でハードウェア プロファイルを使用する方法を示しています。

- 1 ハードウェア プロファイルを作成します。次のいずれかの方法でプロファイルを作成できます。
  - a 新しいプロファイルを作成します。新しいプロファイルの作成方法の詳細については、[ハードウェア プロファイルの作成](#)、(129 ページ) を参照してください。
  - b サーバ上の既存の設定からプロファイルを作成します。サーバ上の既存の設定からプロファイルを作成する方法の詳細については、[既存の設定からのプロファイルの作成](#)、(129 ページ) を参照してください。
- 2 サーバでプロファイルを適用します。プロファイルを適用する方法の詳細については、[ハードウェア プロファイルの適用](#)、(131 ページ) を参照してください。
- 3 プロファイルで、必要に応じて次のオプション作業を実行します。
  - a Edit
  - b Delete
  - c Clone

また、特定のプロファイルにマップされるサーバのリストを表示して、このプロファイルに関連付けられているポリシーの詳細を表示することもできます。これらのタスクの実行方法の詳細については、[ハードウェア プロファイルでの一般タスク](#)、(132 ページ) を参照してください。

## ハードウェア プロファイルの作成

### 手順

- 
- ステップ 1 [Policies] > [Manage Policies and Profiles] を選択します。
  - ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。
  - ステップ 3 [Add] をクリックします。
  - ステップ 4 [Hardware Profile] ダイアログボックスで、作成するプロファイルの名前を [Profile Name] フィールドに入力します。  
既存のサーバ構成を使用する場合は、[Create profile from current configuration of the server] チェックボックスをオンにすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、「[既存の設定からのプロファイルの作成](#)」を参照してください。
  - ステップ 5 Cisco UCS S3260 サーバ用のプロファイルの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。
  - ステップ 6 [Profile Entities] ページで [+] をクリックして、プロファイル エントリを追加します。  
[Delete] アイコンをクリックして、既存のエントリを削除することもできます。
  - ステップ 7 [Add Entry to Profile Name] ダイアログボックスで、[Policy Type] を選択します。
  - ステップ 8 作成済みのポリシーの名前が一覧表示される [Policy Name] ドロップダウンリストからポリシー名を選択します。  
[Policy Name] の横にある [+] をクリックすると、選択したポリシータイプに基づき新しいポリシーを作成できます。ポリシーの作成の詳細については、以下を参照してください。[ハードウェアポリシーの作成](#)、(93 ページ)
  - ステップ 9 [Apply Policy To] ドロップダウンリストからポリシーを適用するサーバを選択します。
  - ステップ 10 [Submit] をクリックします。
  - ステップ 11 [Profile Entities] ページで、[Submit] をクリックします。
- 

### 次の作業

また、プロファイルを編集、削除、複製したり、選択されたプロファイルにマップされるサーバを表示したりできます。これらのタスクの実行については、以下を参照してください。[ハードウェア プロファイルでの一般タスク](#)、(132 ページ)

## 既存の設定からのプロファイルの作成

すでに設定済みのサーバを使用してプロファイルを作成することもできます。サーバ上の既存の設定を再使用すると、類似する設定を作成するのに必要な時間と労力を軽減できます。



(注) サーバの現在の設定からプロファイルを作成するときには、サーバからパスワードフィールドが取得されません。

サーバの現在の設定からプロファイルを作成するには、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Policies] > [Manage Policies and Profiles] を選択します。
- ステップ 2** [Hardware Profiles] タブを選択します。
- ステップ 3** [Add] をクリックします。
- ステップ 4** プロファイルの名前を [Name] フィールドに入力します。
- ステップ 5** [Create profile from current configuration of the server] チェックボックスをオンにします。次の方法でサーバの詳細情報を使用できます。Cisco UCS C3260 サーバの場合はステップ 10 に進みます。
- a) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。
    - 1 [Server IP] フィールドに IP アドレスを入力します。
    - 2 既存のポリシーを選択するために [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウンリストからポリシーを選択するか、[Credential Policy] ドロップダウンリストの横にある [+] をクリックし、[Credential Policy Add Form] ダイアログボックスで詳細を入力して新規ポリシーを作成します。
    - 3 [User Name] フィールドにサーバログイン名を入力します。
    - 4 [Password] フィールドにサーバログインパスワードを入力します。
    - 5 [Protocol] ドロップダウンリストから http または https を選択します。
    - 6 [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。
    - 7 [Select] をクリックし、ポリシーを選択して [Select] をクリックします。
  - b) [Select] をクリックして、設定の取得元となるサーバを選択します。
  - c) [Select] をクリックし、ポリシーを選択して、[Select] をクリックします。
- ステップ 6** [Next] をクリックします。
- ステップ 7** [Profile Entities] ダイアログボックスで [+] をクリックして、プロファイル名にエントリを追加します。  
[Profile Name] テーブルから既存のエントリを削除するには、[x] をクリックします。
- ステップ 8** [Submit] をクリックします。
- ステップ 9** [Submit Result] ダイアログボックスで、[OK] をクリックします。
- ステップ 10** Cisco UCS C3260 サーバの場合は、[Cisco UCS C3260] チェックボックスをオンにして、[Next] をクリックします。
- a) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。

- 1 Cisco UCS C3260 プラットフォームの [Server IP] フィールドに仮想的な管理 IP アドレスを入力します。
  - 2 既存のポリシーを選択するために [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[Credential Policy Add Form] ダイアログボックスで詳細を入力して新規ポリシーを作成します。
  - 3 [User Name] フィールドにサーバ ログイン名を入力します。
  - 4 [Password] フィールドにサーバ ログイン パスワードを入力します。
  - 5 [Protocol] ドロップダウン リストから http または https を選択します。
  - 6 [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。
  - 7 [Select] をクリックし、ポリシーを選択して [Select] をクリックします。
- b) [Select] をクリックして、設定の取得元となるサーバを選択します。
- c) [Select] をクリックし、サーバから作成するポリシーを選択して、[Select] をクリックします。
- ステップ 11** [Next] をクリックします。
- ステップ 12** [Profile Entities] ダイアログボックスで [+] をクリックして、プロファイル名にエントリを追加します。
- [Profile Name] テーブルから既存のエントリを削除するには、[x] をクリックします。
- (注) Cisco UCS C3260 のプロファイルタイプの場合、プラットフォームタイプが Cisco UCS C3260 のポリシーのみ追加できます。ポリシーがコンピューティング ノードタイプの場合、[Apply Policy To] フィールドでサーバ ノードを指定する必要があります。例、[Server-1]、[Server-2]、および [Both]。管理ポリシーの場合、このフィールドは関係ありません。
- ステップ 13** [Submit] をクリックします。
- ステップ 14** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## ハードウェア プロファイルの適用

ハードウェア プロファイルをラック サーバに適用するには、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Policies] > [Manage Policies and Profiles] を選択します。
- ステップ 2** [Hardware Profiles] タブを選択します。
- ステップ 3** 既存のハードウェア プロファイルを選択し、[Apply] をクリックします。

適用 (Apply Profile) ]ダイアログボックスで、プロファイルを適用するサーバまたはシャーシ (Cisco UCS C3260のタイプのプロファイルに適用可能です) を選択できます。これらのオプションを選択したサーバプラットフォームに基づいて表示されます。

- ステップ 4** 自分のプロファイルを適用する[適用 (Profile) ]ダイアログボックスで、[シャーシを選択します。またはサーバ。
- ステップ 5** プロファイルタスクの適用を後でスケジュールするには、[Schedule Later] チェックボックスをオンにします。
- ステップ 6** [Schedule] ドロップダウンリストから既存のスケジュールを選択するか、または[+]をクリックして新しいスケジュールを作成します。スケジュール作成の詳細については、[スケジュールの作成](#)、(143 ページ) を参照してください。
- (注) [Policies]>[Manage Schedules] の順に移動して、スケジュールを選択し、[View Scheduled Tasks] をクリックしてスケジュールされたタスクを表示するか、または[Remove Scheduled Tasks] をクリックしてスケジュールされたタスクを削除できます。
- ステップ 7** [Submit] をクリックします。
- ステップ 8** [Submit Result] 確認ダイアログボックスで、[OK] をクリックします。指定したサーバセットにプロファイルを適用するプロセスが開始します。プロファイルの種類、およびプロファイルが適用されるサーバへのネットワーク接続に応じて、このプロセスに数分かかる場合があります。

## ハードウェア プロファイルでの一般タスク

既存のプロファイルのサーバマッピング詳細を編集、削除、複製、または表示するには、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Policies] > [Manage Policies and Profiles] > [Hardware Profiles] を選択します。
- ステップ 2** 左側ペインの [Hardware Profile] を展開して、[Hardware Profiles] ページで、プロファイルを選択します。オプションで次の作業を行うことができます。
- (任意) プロファイルを削除するには、[Delete] をクリックします。[Delete Profile] ダイアログボックスの [Select] をクリックし、1つ以上のプロファイルを選択して、[Select] をクリックします。[Submit] をクリックするとプロファイルが削除されます。サーバに関連付けられていてもプロファイルを削除できます。
  - (任意) プロファイルを変更するには、プロファイルを選択し、[Edit] をクリックして、必要に応じてプロパティを変更します。プロファイル名を変更するときには、すでに存在する名前を指定しないでください。
  - (任意) 既存のプロファイルの詳細を新しいプロファイルにコピーするには、[Clone] をクリックします。



- d) (任意) サーバまたはサーバグループにプロファイルを適用するには、[Apply]をクリックします。プロファイルを適用する方法の詳細については、[ハードウェアプロファイルの適用](#)、(131 ページ) を参照してください。
- e) (任意) [View Details] をクリックすると、すでに適用したプロファイルのステータス、およびプロファイルが適用されたサーバ IP アドレスが表示されます。プロファイルが正常に適用されない場合、[Status Message] 列にエラーメッセージが表示されます。

**ステップ 3** 状況に応じて [Submit] または [Close] をクリックします。

## タグライブラリ

オブジェクトにラベルを割り当てる場合にタグ付けを行います。管理者は、Cisco IMC Supervisor のリソースグループやユーザグループなどのオブジェクトにタグを付けることを決定できます。ラック アカウントなどのカテゴリにタグを割り当てることができます。また、選択したカテゴリの特定のタイプのアカウントにタグを適用することもできます。

[Tag Library] の唯一のタブには、次の詳細が表示されます。

フィールド	説明
[Name]	タグライブラリのユーザ定義名。
[Description]	タグライブラリのユーザ定義の簡単な説明。
[Type]	文字列または整数。
[Possible Tag Values]	ユーザ定義のタグ値。
[Applies To]	ラックマウント サーバまたはユーザ。

## タグライブラリの作成

タグライブラリを作成する場合は、次の手順を実行します。

### 手順

- ステップ 1** メニューバーで、[Policies] > [Tag Library] を選択します。
- ステップ 2** [Create] をクリックします。
- ステップ 3** [Create Tag] ダイアログボックスで、[Tag Details] の次のフィールドに入力します。

フィールド	説明
[Name] フィールド	タグの記述名。
[Description] フィールド	(オプション) タグの説明。
[Type] ドロップダウン リスト	文字列または整数を選択します。
[Possible Tag Values] フィールド	タグに使用できる値。

**ステップ 4** [Next] をクリックします。

**ステップ 5** [Applicability Rules] ペインで、次の手順を実行します。

名前	説明
[Taggable Entities] フィールド	<p>タグを適用する必要があるエンティティを選択します。</p> <p>エンティティを追加するには、以下を実行します。</p> <ol style="list-style-type: none"> <li>1 [+] アイコンをクリックします。</li> <li>2 [Category] ドロップダウンリストから、カテゴリを選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• [Physical_Compute]</li> <li>• [Administration]</li> </ul> </li> <li>3 テーブルからタグ付け可能なエンティティを選択します。</li> <li>4 [Submit] をクリックします。</li> </ol> <p>(注) タグは、タグ付け可能なエンティティの設定に応じてそれぞれのカテゴリの下に表示されます。</p>

**ステップ 6** 確認ダイアログボックスで、[OK] をクリックします。

**ステップ 7** [Create Tag] ダイアログボックスで、[Submit] をクリックします。

**ステップ 8** [OK] をクリックします。

(注) 使用可能なオプションをクリックすることで、タグおよびタグの関連付けの詳細を複製、編集、削除、表示するといった、さまざまなタスクを実行できます。



## 第 9 章

# ファームウェア プロファイル

この章は、次の内容で構成されています。

- [ファームウェア管理メニュー, 135 ページ](#)

## ファームウェア管理メニュー

ファームウェア イメージは、ローカル サーバまたはネットワーク サーバからアップロードできます。プロファイル名は、ローカルおよびネットワークの両方のイメージプロファイルの間で一意的である必要があります。

シスコは、すべての Cisco IMC Supervisor コンポーネントをアップグレードするためのファームウェアのアップデートをまとめて提供します。ファームウェアのアップデートは、[cisco.com](#) からダウンロードできます。サーバが Cisco IMC Supervisor で管理されていない場合はアップグレードできません。E シリーズファームウェアイメージをダウンロードするには、[cisco.com](#) アカウントへの契約アクセスの関連付けを行う必要があります。

## ローカル サーバへのイメージの追加

ローカル マシンからファームウェア イメージを追加するには、次の手順を実行します。

### 手順

- ステップ 1 [Systems] > [Firmware Management] を選択します。
- ステップ 2 [Images - Local] タブをクリックし、[+] をクリックしてイメージを追加します。
- ステップ 3 [Add Firmware Image - Local] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Profile Name] フィールド	プロファイルを記述する一意の名前を入力します。

フィールド	説明
[Enable Proxy Configuration] チェックボックス	<p>(任意) このチェックボックスは、設定したプロキシ設定の詳細を取得します。</p> <p>(注) すでに設定している Cisco.com のユーザクレデンシヤルとプロキシ設定の詳細が自動的に取得されます。Cisco.com クレデンシヤルの設定については <a href="#">Cisco.com ユーザの設定, (38 ページ)</a> を参照し、プロキシ設定については <a href="#">プロキシの設定, (38 ページ)</a> を参照してください。</p>
[Platform] ドロップダウン リスト	ドロップダウン リストからプラットフォームを選択します。少なくとも1つのサーバを管理するプラットフォームだけがここにリストされます。
[Available Image] ドロップダウン リスト	ドロップダウン リストから .iso イメージを選択します。
[Download Now] チェックボックス	プロファイルの追加後、ただちに .iso イメージをダウンロードするには、このチェックボックスをオンにします。そうでない場合は、[Download Image] をクリックして、後でイメージをダウンロードすることができます。
[Accept License Agreement]	<p>ライセンス契約書に同意するには、このチェックボックスをオンにします。[Terms and Conditions] リンクをクリックすると、エンドユーザライセンス契約書を確認できます。</p> <p>(注) ライセンス契約書に合意しない場合、イメージを後でダウンロードする予定であっても、ファームウェア プロファイルを作成することはできません。</p>

**ステップ 4** [Submit] をクリックします。

**ステップ 5** [Submit Result] ダイアログボックスで、[OK] をクリックします。

- (注)
- プロファイル設定の詳細を表示し、ファームウェア イメージの詳細を変更し、イメージ プロファイルを削除できます。同時に複数のプロファイルを選択して削除することもできます。
  - Cisco IMC Supervisor アプライアンスが、これらのイメージにリモートでマッピングできる必要があります。
  - [Images-Local] ウィンドウからイメージを選択し、cisco.com からイメージをダウンロードできます。イメージのダウンロードが必要になるファームウェア プロファイルの場合は、[Download Image] オプションを使用してダウンロードプロセスを延期し、後で開始することができます。また、[Delete Image] オプションを使用して、cisco.com からダウンロードしたイメージを削除することもできます。

## ローカル ファイル システムからのイメージのアップロード

ローカル ファイル システムから Cisco IMC Supervisor システムに ISO イメージをアップロードするには、次の手順を実行します。

### 手順

- ステップ 1** メニュー バーで、[Systems] > [Firmware Management] を選択します。
- ステップ 2** [Images - Local] タブをクリックし、[Upload] をクリックしてイメージを追加します。
- ステップ 3** [Upload Firmware Image - Local] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Profile Name] フィールド	プロファイルを記述する一意の名前を入力します。
[Platform] ドロップダウン リスト	CシリーズまたはEシリーズプラットフォームを選択します。
[File Name] フィールド	ローカル ファイル システムでアップロードするファイルを検索して選択するには、[Browse] を選択します。

- ステップ 4** [Upload] をクリックします。
- ステップ 5** アップロードが完了したら、[File Upload] 確認ダイアログ ボックスで [OK] をクリックします。
- ステップ 6** [Submit] をクリックします。
- (注)
- プロファイル設定の詳細を表示し、ファームウェア イメージの詳細を変更し、イメージプロファイルを削除できます。同時に複数のプロファイルを選択して削除することもできます。
  - [Delete Profile] オプションを使用すると、プロファイルに関連付けられたイメージを削除できます。誤ったイメージをアップロードしたり、ファイルがプロファイルに関連付けられていない場合は、定期的に（月に1回）実行されるシステム消去タスクによって、Cisco IMC Supervisor アプライアンスからファイルが削除されます。

## ネットワーク サーバからのイメージの追加

プロファイル名、リモートIP、リモートファイル名などを提供することで、ネットワークサーバからファームウェア イメージを追加するには、次の手順を実行します。

## 手順

- ステップ 1** メニュー バーで、[Systems] > [Firmware Management] を選択します。
- ステップ 2** [Images - Network] タブをクリックし、[+] をクリックしてイメージを追加します。
- ステップ 3** [Add Firmware Image - Network] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Profile Name] フィールド	プロファイルを記述する一意の名前。プロファイル名は固有である必要があります。
[Platform] ドロップダウン リスト	ドロップダウン リストからプラットフォームを選択します。少なくとも1つのサーバを管理するプラットフォームだけがここにリストされます。
[Server Type] ドロップダウン リスト	ネットワーク ファイルシステム (NFS)、Common Internet File System (CIFS) または HTTP/S サーバタイプを選択します。
[Remote IP] フィールド (NFS および CIFS サーバタイプの場合のみ)	リモート IP アドレスを入力します。
[Remote Share] フィールド (NFS および CIFS サーバタイプの場合のみ)	リモート共有パスを入力します。
[Remote File Name] フィールド (NFS および CIFS サーバタイプの場合のみ)	リモート ファイル名を入力します。 (注) リモート ファイル名は Host Upgrade Utility ISO ファイルです。
[Location Link] フィールド (HTTP サーバタイプの場合のみ)	イメージの場所の有効な http または https URL リンクを入力します。
[User Name] フィールド	ネットワーク パスのユーザ名を入力します。
[Password] フィールド	ネットワーク パスのパスワードを入力します。
[Mount Options] ドロップダウン リスト (CIFS サーバタイプの場合のみ)	[Mount Options] ドロップダウン リストから、有効なマウント オプションを選択します。 (注) Cisco IMC バージョン 2.0(8) 以降を実行しているサーバ用にマウント オプションを選択できます。

**ステップ 4** [Submit] をクリックします。

**ステップ 5** [Submit Result] ダイアログボックスで、[OK] をクリックします。

- (注)
- プロファイル設定の詳細を表示し、ファームウェア イメージの詳細を変更し、イメージプロファイルを削除できます。同時に複数のプロファイルを選択して削除することもできます。
  - Cisco IMC Supervisor アプライアンスが、これらのイメージにリモートでマッピングできる必要があります。

## ファームウェアのアップグレード

### はじめる前に

Cisco IMC バージョン 2.0(x) にアップグレードする場合、デフォルトの Cisco IMC パスワードを変更する必要があります。



(注) 単一の Cisco UCS C3260 高密度ストレージラック サーバシャーシの一部である両方のサーバを同時にアップグレードすることは推奨されません。

Cisco IMC Supervisor をアップグレードする前に、ファームウェア プロファイルがすでに設定されている場合は、CCO クレデンシャルとプロキシの詳細が設定されていることを確認してください。設定については、[Cisco.com ユーザの設定](#)、[\(38 ページ\)](#) および [プロキシの設定](#)、[\(38 ページ\)](#) を参照してください。

### 手順

**ステップ 1** メニュー バーで、[Systems] > [Firmware Management] を選択します。

**ステップ 2** [Firmware Upgrades] タブをクリックします。

**ステップ 3** [Run Upgrade] をクリックします。

警告メッセージが表示され、選択したサーバのアップグレードを実行すると、ホストがリブートしてファームウェアのアップデート ツールが起動することが通知されます。ファームウェアのアップデートが完了すると、サーバがリブートして元のホスト OS が起動します。

**ステップ 4** [OK] をクリックして確定します。

**ステップ 5** [Upgrade Firmware] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Select Profile] ドロップダウン リスト	ドロップダウン リストからプロファイルを選択します。

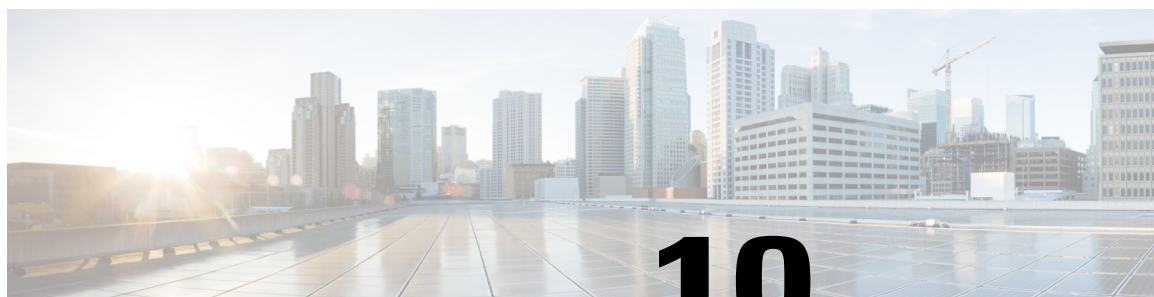
フィールド	説明
[Platform]	サーバプラットフォーム、ファームウェアイメージのバージョン、選択したファームウェアプロファイルのパスなどの詳細を表示できます。
[Image Version]	
[Image Path]	
[Server(s)] ボタン	[Select] をクリックして、リストからサーバを選択します。選択したプロファイルで設定されているプラットフォームに一致するサーバだけがリストに表示されます。
[Schedule later] チェックボックス	このチェックボックスをオンにして、アップグレードを実行する既存のスケジュールを選択します。[+] アイコンをクリックして新しいスケジュールを作成することもできます。スケジュール作成の詳細については、 <a href="#">スケジュールの作成, (143 ページ)</a> を参照してください。[Policies]>[Manage Schedules] の順に移動してスケジュールを選択し、[View Scheduled Tasks] をクリックしてスケジュールされたタスクとその進行状況を確認できます。また、スケジュールされたタスクを選択し、[Remove Scheduled Tasks] をクリックして、関連付けられているスケジュール済みタスクを削除することもできます。

**ステップ 6** [Upgrade Firmware] ダイアログボックスで、[Submit] をクリックします。

**ステップ 7** [OK] をクリックします。

(注) ファームウェア アップグレードの詳細を表示したり、指定したアップグレード操作のステータス レコードを削除することもできます。





# 第 10 章

## Cisco IMC Supervisor の更新

この章は、次の内容で構成されています。

- [Cisco IMC Supervisor パッチの更新の概要](#), 141 ページ
- [Cisco IMC Supervisor パッチ更新の確認](#), 141 ページ

### Cisco IMC Supervisor パッチの更新の概要

自動パッチ更新通知は Cisco IMC Supervisor で使用できます。Cisco IMC Supervisor は、シスコの自動ソフトウェア配布 (ASD) サービスを使用して、[cisco.com](http://cisco.com) で使用可能な新しいパッチ更新の有無を定期的に (14 日ごとに) 確認します。現在のリリース以降のパッチ更新があれば、Cisco IMC Supervisor 更新マネージャーによってパッチが Cisco IMC Supervisor 内の場所にダウンロードされます。たとえば、[Location] に `/opt/infra/uploads/external/downloads/imcs/<filename.zip>` と表示されている場合は、パッチ URL に `file:///opt/infra/uploads/external/downloads/imcs/<filename.zip>` ftp コマンドを使用できます。その後、Shell Admin に移動して、パッチを適用できます。パッチの適用に関する詳細については、『[Cisco IMC Supervisor Shell Guide](#)』の「[Applying a Patch to Cisco IMC Supervisor](#)」の項を参照してください。[Check For Updates Now] オプションを使用して、新しいバージョンが使用可能か手動で確認することもできます。



(注) 現在のリリースの新しいパッチ更新のみが通知されます。Cisco IMC Supervisor ベースの更新は OVF ファイルには適用されません。

### Cisco IMC Supervisor パッチ更新の確認

Cisco IMC Supervisor に新しいパッチ更新の有無について定期的に (14 日ごとに) チェックを実行させるには、サポートクレデンシャルとその他の詳細を入力する必要があります。これらの詳細が Cisco IMC Supervisor によって使用され、Cisco ASD のバックエンドサービスと通信して、新し

い更新について問い合わせを行います。パッチの新しいバージョンは、Cisco IMC Supervisor アプライアンスに自動的にダウンロードされます。

## 手順

---

- ステップ 1** メニュー バーで、[Administration] > [Update IMCS] を選択します。  
[IMCS Update Report] に、現在のバージョン、利用可能なアップグレードバージョン、アップグレードステータス、ファイルがダウンロードされている場所などが表示されます。  
(注) Cisco IMC Supervisor アプライアンスからホスト名 `cloudsso.cisco.com` および `api.cisco.com` にアクセスできることを確認します。
- ステップ 2** [Check For Updates Now] アイコンをクリックして、Cisco IMC Supervisor 更新の有無を確認します。
- ステップ 3** [Submit] をクリックします。  
レポートに最新の更新が表示されます。
- ステップ 4** [Export Report] アイコンをクリックして、レポートを PDF、CSV、または XLS 形式でエクスポートします。
- ステップ 5** [Generate Report] をクリックします。
- ステップ 6** [Download] をクリックしてレポートをダウンロードするか、または [Close] をクリックします。
-



# 第 11 章

## スケジュールの管理

この章は、次の内容で構成されています。

- [スケジュール管理の概要, 143 ページ](#)
- [スケジュールの作成, 143 ページ](#)

### スケジュール管理の概要

スケジュールを定義することで、特定のタスクを異なるタイミングで発生するように保留することができます。たとえば、ファームウェアのアップデート、サーバ検出、ポリシーおよびプロファイルの適用などのタスクを事前に定義した時刻または事前に定義した頻度で実行するようにスケジュールできます。サーバの作業負荷が低いオフピーク時にタスクをスケジュールできます。

### スケジュールの作成

新しいスケジュールを作成するには、次の手順を実行します。

#### 手順

- ステップ 1 メニューバーで、[Policies] > [Manage Schedules] を選択します。
- ステップ 2 [Add] をクリックします。
- ステップ 3 [Create Schedule] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Schedule Name] フィールド	スケジュール タスクの名前を入力します。

フィールド	説明
[Enable Schedule] チェックボックス	スケジュールを有効にするには、このチェックボックスをオンにします。スケジュールを有効または無効にすることにより（[Enable] または [Disable] オプションを使用）、スケジュールに関連付けられているタスクの実行を有効または無効にできます。
[Scheduler Type] オプション ボタン	<p>1 回限りのスケジュールか、繰り返しのスケジュール間隔を選択します。</p> <p>[One Time] スケジュールを選択した場合は、日付、時刻、および AM または PM のオプションボタンを選択します。</p> <p>(注) スケジュールの時刻はアプライアンスの時刻に基づいています。ただし、タイムゾーンはローカルクライアントブラウザに基づきます。</p> <p>[Recurring] スケジュールを選択した場合は、日数（0～30 日）、時間と分数をドロップダウンリストから選択します。</p>

ステップ 4 [Submit] をクリックします。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] をクリックします。

### 次の作業

- 既存のスケジュールを選択し、スケジュール済みタスクの変更、削除、確認ができます。  
[View Scheduled Tasks] には、ファームウェアのアップグレード、自動検出のステータスを確認できるレポートが表示されます。また、「[ファームウェアのアップグレード](#)」、「[自動検出の実行](#)」、[ハードウェアポリシーの適用](#)、(126 ページ)、または [ハードウェアプロファイルの適用](#)、(131 ページ) で、スケジュールに関連付けられた適用ポリシーやプロファイルタスクのステータスを確認できるレポートも表示されます。
- スケジュールに関連付けられている タスク（複数可）を選択し、[Remove Scheduled Tasks] オプションを使用して、スケジュールとの関連を解除できます。



## 第 12 章

# サーバ診断の実行

この章は、次の内容で構成されています。

- [サーバ診断の概要, 145 ページ](#)
- [サーバ設定ユーティリティ イメージの場所の設定, 146 ページ](#)
- [診断の実行, 147 ページ](#)

## サーバ診断の概要

サーバ診断は、UCS サーバ設定ユーティリティ (UCS-SCU) から使用できます。診断ツールを使用して、シスコサーバのハードウェア問題を診断し、さまざまなサーバコンポーネントに対してテストを実行し、ハードウェアの問題を見つけたり、テスト結果を表形式で分析することができます。

UCS-SCU イメージをダウンロードおよび設定し、リモート ロケーションに保存する必要があります。



(注) UCS-SCU イメージを使用して診断テストを実行すると、サーバが UCS-SCU イメージで再起動されるので、サーバが一時的に使用できなくなります。

Cisco IMC Supervisor 能力がサーバがある、地理的な場所で設定されている複数の診断イメージを持つことがあります。これとせずと早く実行する診断は、その場所内のサーバとイメージの間の低遅延ネットワークが容易になります。

任意のラックサーバで診断を実行すると、そのサーバは設定した場所でホストされている UCS-SCU イメージでリブートされます。診断の表形式のレポートには、診断を実行した各サーバに関する診断のステータスが表示されます。また、サーバの詳細、レポートが生成された日時、診断ステータスなども表示されます。単一または複数のサーバに関する診断レポートを削除したり、ダウンロードしたりできます。



(注) サーバ診断を実行するには、`scpuser` パスワードを設定する必要があります。`scpuser` パスワードを設定するには、[SCP ユーザの設定](#)、(36 ページ) を参照してください。

## サーバ設定ユーティリティ イメージの場所の設定

UCS-SCU イメージの場所を設定して保存するには、次の手順を実行します。

### 手順

- ステップ 1** メニューバーから、[Systems] > [Server Diagnostics] を選択します。
- ステップ 2** [SCU Image Profiles] をクリックします。
- ステップ 3** [Configure SCU Image Location] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Profile Name] フィールド	プロファイルの記述名。
[ISO Share Type] ドロップダウンリスト	[Network File System (NFS)]、[Common Internet File System (CIFS)]、[World Wide Web (WWW)]、または [LOCAL] 共有タイプを選択します。
[LOCAL] を選択する場合	
[SCU Image] フィールド	SCU イメージファイルを参照、選択、およびアップロードします。
[NFS]、[CIFS]、または [WWW (HTTP/HTTPS)] を選択する場合	
[ISO Share IP] フィールド	ISO 共有 IP アドレスを入力します。
[ISO Share Path] フィールド	ISO 共有パスを入力します。
[Username] フィールド	ISO 共有ログイン ユーザ名を入力します。
[Password] フィールド	ISO 共有ログイン パスワードを入力します。

- ステップ 4** [Save] をクリックします。
- ステップ 5** [Submit Result] ダイアログボックスで、[OK] をクリックします。

## 診断の実行

サーバまたはサーバグループの診断を実行するには、次の手順を実行します。

### 手順

**ステップ 1** メニューバーから、[Systems] > [Server Diagnostics] を選択します。

**ステップ 2** [Run Diagnostics] をクリックします。

**ステップ 3** [Run Diagnostics] ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Select Profile] ドロップダウンリスト	ドロップダウンリストから、既存のプロファイルを選択します。
[Choose] ドロップダウンリスト	ドロップダウンリストから、診断をサーバで実行するかサーバグループで実行するかを選択します。
[Server(s)] または [Server Group(s)] ドロップダウンリスト	診断を実行するサーバまたはサーバグループを選択します。

**ステップ 4** [Select] をクリックし、[Select] ダイアログボックスからサーバまたはサーバグループを選択します。

**ステップ 5** [Select] をクリックします。  
選択したサーバまたはサーバグループは、[Server(s)] または [Server Group(s)] フィールドの横に表示されます。

**ステップ 6** [Submit] をクリックします。

**ステップ 7** [Submit Result] ダイアログボックスで、[OK] をクリックします。  
(注) サーバもしくは複数のサーバ上で次のアクションを実行できます。

- レポートを表示するには、サーバを選択して、[View Report] をクリックします。
- レポートを削除するには、1つ以上のサーバを選択して、[Delete Report] をクリックします。
- レポートをダウンロードするには、1つ以上のサーバを選択して、[Download Report] をクリックします。診断レポートをダウンロードするために複数のサーバを選択した場合は、すべてのレポートを含む zip ファイルがダウンロードされます。
- すでに診断操作を実行しているサーバは選択できません。そのサーバで別の診断をトリガーするには、診断操作が完了するまで待ちます。
- 診断が終了するまでに約 40 分かかる場合があります。これは、サーバに存在するコンポーネントの数によって異なります。







# 第 13 章

## Cisco IMC Supervisor 向け Smart Call Home

この章は、次の内容で構成されています。

- [Smart Call Home の概要](#), 149 ページ
- [Smart Call Home の設定](#), 149 ページ
- [障害コード](#), 150 ページ

### Smart Call Home の概要

Cisco Smart Call Home は、選択されたシスコ デバイスで継続的なモニタリング、プロアクティブな診断、アラート、修復案を提供する自動サポート機能です。Smart Call Home は、問題を迅速に特定および解決し、高可用性と業務の効率化の向上を実現するために役立ちます。この機能は、Cisco IMC Supervisor によって管理されているハードウェアに有効なサポート契約があれば使用できます。有効な場合、Smart Call Home が、シスコが Cisco Technical Assistance Center (TAC) のエンジニアやシスコサポートコミュニティおよび開発者とやりとりして識別した特定の障害について確認します。ユーザが問題または障害に気づいてエスカレーションや報告するのを待つのではなく、Smart Call Home が障害を事前に特定し、診断します。

グループ ラック サーバ インベントリ、ラック サーバ 障害、ヘルス システム など、Cisco IMC Supervisor が管理するサーバ タスクは、定期的に行われ、関連情報を Smart Call Home のバックエンドに送信します。バックエンドはこのデータを処理し、問題が確認された場合は、問題解決のために TAC を使用して自動的にケースが上げられます。

Cisco IMC Supervisor ユーザ インターフェイスを使用して Smart Call Home を設定できます。詳細については、[Smart Call Home の設定](#), (149 ページ) を参照してください。

### Smart Call Home の設定

Smart Call Home を設定するには、次の手順を実行します。

## 手順

- 
- ステップ 1** メニューバーから、[Administration] > [System] > [Smart Call Home] の順に選択します。
- ステップ 2** 収集された障害が Smart Call Home のバックエンドに転送されるように、[Enable Smart Call Home] チェックボックスをオンにします。  
 (注) デフォルトでは、Smart Call Home は無効になっています。
- ステップ 3** [Contact Email] アドレスを入力します。  
 (注) このフィールドに一度に入力できる連絡先電子メールは 1 つだけです。
- ステップ 4** Smart Call Home のバックエンドの [Destination URL] はデフォルトで設定されます。  
 (注)
  - デフォルトの URL は変更しないことを推奨します。
  - デフォルトでは、[Enable Proxy] チェックボックスはオンになっています。Smart Call Home は、すでに設定されているプロキシの詳細を使用します。プロキシの設定方法については、[プロキシの設定](#)、(38 ページ) を参照してください。
- ステップ 5** (オプション) サーバのインベントリの詳細を送信するには、[Send Group Inventory Now] チェックボックスをオンにします。管理対象サーバごとに 1 つのインベントリ メッセージが Smart Call Home のバックエンドに送信されます。これは、TAC チームによる問題解決のための追加情報として使用されることがあります。
- ステップ 6** [Save] をクリックします。  
 (注)
  - 管理対象サーバで発生した障害はバックエンドに送信されます。さまざまな障害コードと重大度については、[障害コード](#)、(150 ページ) を参照してください。Smart Call Home にログインし、さまざまなタスクを実行する方法についての詳細は <https://supportforums.cisco.com/community/4816/smart-call-home> を参照してください。Smart Call Home のバックエンドで受信したメッセージを表示する方法についての詳細は <http://tools.cisco.com/sch/> を参照してください。
  - URL <https://tools.cisco.com/its/service/oddce/services/DDCEService> が Cisco IMC Supervisor アプライアンスから到達可能であることを確認します。
- 

## 障害コード

以下は、Cisco IMC Supervisor が Smart Call Home のバックエンドに送信するエラー メッセージのリストです。

障害コード	障害名	メッセージ	重大度
F0174	fltProcessorUnitInoperable	Processor [id] on [serverId] operability: [operability]	critical major
F0181	fltStorageLocalDiskInoperable	Local disk [id] on [serverid] operability: [operability]	major warning
F0185	fltMemoryUnitInoperable	DIMM [location] on [serverid] operability: [operability]	major
F0407	fltEquipmentPsuIdentity	Power supply [id] on [serverid] has a malformed FRU	critical
F0531	fltStorageRaidBatteryInoperable	RAID Battery on [serverid] operability: [operability]	major
F0997	fltStorageRaidBatteryDegraded	Raid battery [id] on [serverid] operability: [operability]	major
F1004	fltStorageControllerInoperable	Storage Controller [id] operability: [operability]	critical
F1007	fltStorageVirtualDriveInoperable	Virtual drive [id] on [serverid] operability: [operability]	critical
F0379	fltEquipmentIOCardThermalProblem	IOCard [location] on server [id] operState: [operState]	major
F0385	fltEquipmentPsuThermalThresholdNonRecoverable	Power supply [id] in [serverid] temperature: [thermal]	critical
F0389	fltEquipmentPsuVoltageThresholdCritical	Power supply [id] in [serverid] voltage: [voltage]	major
F0391	fltEquipmentPsuVoltageThresholdNonRecoverable	Power supply [id] in [serverid] voltage: [voltage]	critical

障害コード	障害名	メッセージ	重大度
F0411	fltEquipmentChassisThermalThresholdNonRecoverable	Thermal condition on [serverid] cause: [thermalStateQualifier]	critical
F0424	fltComputeBoardCmosVoltageThresholdCritical	CMOS battery voltage on [serverid] is [cmosVoltage]	major
F0425	fltComputeBoardCmosVoltageThresholdNonRecoverable	CMOS battery voltage on [serverid] is [cmosVoltage]	critical
F0868	fltComputeBoardPowerFail	Motherboard of [serverid] power: [power]	critical
F0176	fltProcessorUnitThermalThresholdCritical		major
F0177	fltProcessorUnitThermalThresholdNonRecoverable	Processor [id] on [serverid] temperature:[thermal]	critical
F0187	fltMemoryUnitThermalThresholdCritical		major
F0188	fltMemoryUnitThermalThresholdNonRecoverable	DIMM [location] on [serverid] temperature: [thermal]	critical
F0312	fltComputePhysicalThermalProblem		major



## 第 14 章

# Cisco UCS C3260 高密度ストレージラック サーバの管理

この章は、次の内容で構成されています。

- [Cisco UCS C3260 高密度ストレージラック サーバについて, 153 ページ](#)
- [Cisco UCS C3260 高密度ストレージラック サーバアーキテクチャの概要, 154 ページ](#)
- [Cisco UCS C3260の高密度ストレージラック サーバでCisco IMCスーパーバイザ, 155 ページ](#)
- [ラック アカウントの追加, 156 ページ](#)
- [Cisco UCS C3260 ラック サーバの管理, 156 ページ](#)
- [ポリシーとプロファイル, 158 ページ](#)
- [ファームウェアのアップグレード, 160 ページ](#)
- [Cisco UCS C3260 高密度ストレージラック サーバの詳細情報の表示, 160 ページ](#)

## Cisco UCS C3260 高密度ストレージラックサーバについて

Cisco UCS C3260 は、デュアルサーバノードをサポートする高密度ストレージラックサーバです。また、ビッグデータ、クラウド、オブジェクトストレージ、コンテンツデリバリなどの環境で使用される大規模データセット用に1つのサーバを最適化することもできます。Cisco UCS C3260 は、Cisco UCS C シリーズラックマウントサーバ製品ファミリに属しています。

Cisco UCS C3260 高密度ストレージラックサーバは、スタンドアロン環境で、Cisco IMC Supervisor と統合された Cisco Unified Computing System の一部として動作するように設計されています。Cisco UCS C3260 高密度ストレージラックサーバには、次の特長があります。

- 冗長ディスクアレイ (RAID) および Just a Bunch Of Disks (JBOD) の全機能とのエンタープライズクラスの冗長性
- スタンドアロンの管理インターフェイス (Cisco Integrated Management Controller)

- サーバノードの交換やアップグレード時にデータ移行が不要
- 奥行きが深いラックが不要

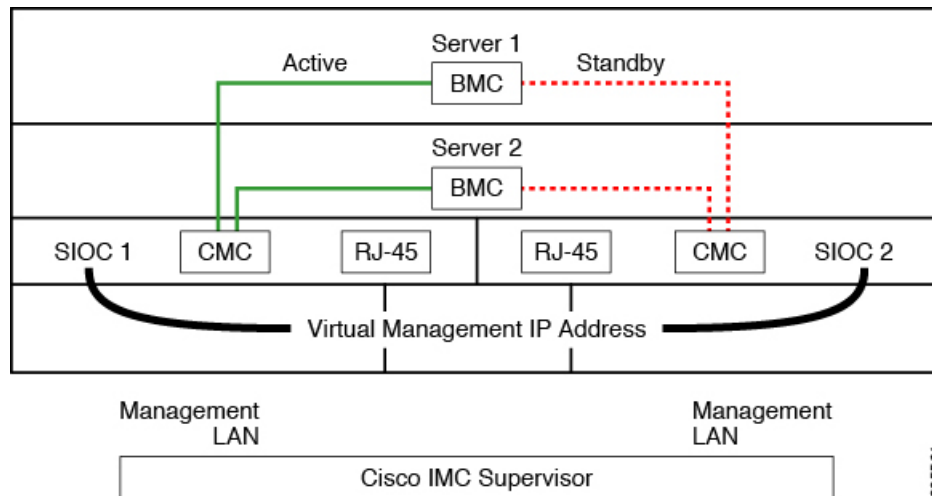
Cisco UCS C3260 高密度ストレージラック サーバの詳細については、[Cisco UCS C3260 ラックサーバ \(Cisco UCS C3260 Rack Server\)](#) を参照してください。

## Cisco UCS C3260 高密度ストレージラック サーバアーキテクチャの概要

### アーキテクチャの概要

Cisco UCS C3260 はシスコのブレードテクノロジーに関する専門知識を生かしたモジュラサーバアーキテクチャを採用しており、別のシステムにデータを移行することなく、システム内のコンピューティングノードやネットワークノードをアップグレードできます。次の機能を備えています。

- デュアルサーバノード
- サーバノードあたり最大 24 のコンピューティングコア
- サーバノードあたり最大 60 台の混合ドライブ (Large Form Factor (LFF) と最大 14 台のソリッドステートディスク (SSD) ドライブ、および 2 台の SSD SATA ブートドライブ)
- サーバノードあたり最大 512 GB のメモリ (合計 1 テラバイト [TB])
- 12 Gbps の Serial Attached SCSI (SAS) ドライブのサポート
- デュアルポート 40 Gbps をサポートする、Cisco VIC 1300 シリーズのチップを内蔵したシステム I/O コントローラ
- ツール不要なサーバノード、システム I/O コントローラ、使いやすいラッチ構造、ホットスワップおよびホットプラグ可能なコンポーネントで実現する高い信頼性、可用性、有用性 (RAS) の機能



このシステムは、シャーシ管理コントローラ（CMC）を使用してサーバノードを管理します。各システム I/O コントローラ（SIOC）モジュールには、内蔵型 CMC が組み込まれています。2つの SIOC を使用する場合、2つの CMC がアクティブ/スタンバイ構成で機能します。Cisco IMC インターフェイスでログインしている SIOC 内の CMC がアクティブ CMC になります。アクティブ CMC を使用して、両方のサーバノードの BMC を管理できます。

Cisco IMC インターフェイスを使用してサーバノードの BMC を管理するためにシステムに接続する場合、SIOC 上の管理ポート（RJ-45）に物理的に接続することになります。Cisco IMC インターフェイスでログインするときは、その SIOC 内の CMC に割り当てられている仮想的な管理 IP アドレスを使用します。

すべてのユーザインターフェイスは、アクティブ CMC でのみ動作します。構成の変更は、アクティブ CMC とスタンバイ CMC の間で自動的に同期されます。

システムの電源を再投入すると、デフォルトで SIOC 1 内の CMC がアクティブ CMC になります。次のいずれかの条件が発生すると、アクティブ CMC はスタンバイ CMC にフェールオーバーします。

- アクティブ CMC のリブートまたは障害が発生した場合。
- アクティブ CMC を持つ SIOC が取り外された場合。
- アクティブ CMC でネットワーク接続が失われた場合。

C3260 ラックサーバの設定については、[Cisco UCS C3260 ラックサーバの仕様シート（Cisco UCS C3260 Rack Server Specification Sheet）](#) を参照してください。

## Cisco UCS C3260の高密度ストレージラックサーバでCisco IMCスーパーバイザ

Cisco IMCのスーパーバイザマネージド高密度ストレージラックサーバはCシリーズラックサーバとともにすべての機能をサポートします。また、これらの機能に追加のレポートを提供し、概念は、次の項で詳細述べられます。

- 概要—Cisco IMCのスーパーバイザを通じてマネージド、Cisco UCS C3260のアーキテクチャに関する詳細情報、および接続を提供します。
- ラック アカウントの追加—説明し、Cisco UCS 3260 シャーシラック アカウントの追加についての詳細情報が表示されます。
- シャーシの管理—説明し、高密度ストレージラック シャーシの構文に関する詳細情報が表示されます。
- ポリシーとプロファイル—説明し、Cisco UCSの詳細情報が3260シャーシポリシーと関連プロファイル提供します。
- ファームウェア アップグレード—Cisco UCS C3260のシャーシファームウェアのパッケージと、ファームウェアが手動で更新できるエンドポイントに関する詳細情報が表示されます。
- 表示のCisco UCS C3260ラックサーバの詳細—PSUs、VICアダプタ、シャーシの概要とSAS展開などの詳細を表示します。

## ラック アカウントの追加

ラック アカウントを追加するために、[Server IP] フィールドに仮想的な管理 IP を指定することができます。ラック アカウントの詳細については、[ラック アカウントの追加](#)、(58 ページ) を参照してください。Cisco UCS C3260 ラックサーバによって管理されているサーバは、インベントリ収集後に [Rack Servers] タブで確認できます。



(注) CMC 1 または CMC 2 IPアドレスを追加すると、エラーが発生します。

## Cisco UCS C3260 ラック サーバの管理

### シャーシ管理コントローラの再起動

#### 手順

- ステップ 1 メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2 右側のペインで、[Chassis] タブを選択します。
- ステップ 3 [Reboot CMC] をクリックします。
- ステップ 4 [Reboot Chassis Management Controller] ダイアログボックスで、[CMC1] または [CMC2] を選択します。
- ステップ 5 [Submit] をクリックします。
- ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。



選択したシャーシが再起動します。

## Cisco UCS C3260 ラック サーバの前面ロケータ LED の設定

サーバロケータ LED を使用すると、データセンター内の多数のサーバ間で特定のサーバを識別できます。選択したシャーシの前面ロケータ LED を点灯または消灯するには、次の手順を実行します。

### 手順

- ステップ 1 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2 右側のペインで、[Chassis] タブを選択します。
- ステップ 3 [Front Locator LED] をクリックします。
- ステップ 4 [Turn the Front Locator LED for selected chassis on/off] ドロップダウンリストから、[ON] または [OFF] を選択します。
- ステップ 5 [Submit] をクリックします。
- ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

## Cisco UCS C3260 ラック サーバのタグの管理

タグgingは、リソースグループ、Cisco UCS C3260 高密度ストレージラック サーバ、またはラックマウントサーバなどのオブジェクトにラベルを割り当てるために使用されます。タグは、ラックの位置、担当サポートグループ、目的、またはオペレーティングシステムなどの情報を提供するために使用できます。Cisco UCS C3260 高密度ストレージラック サーバまたはラックマウントサーバのタグの追加または変更の詳細については、[ラックマウントサーバのタグの管理](#)、(80 ページ) を参照してください。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

## Cisco UCS C3260 ラック サーバのタグの追加

タグgingは、リソースグループまたはラックサーバなどのオブジェクトにラベルを割り当てるために使用されます。タグは、ラックの位置、担当サポートグループ、目的、またはオペレーティングシステムなどの情報を提供するために使用できます。Cisco UCS C3260 ラック サーバにタグを追加するには、次の手順を実行します。

### はじめる前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。



(注) 複数のラック サーバを選択することもできます。

### 手順

- ステップ 1 メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2 右側のペインで、[Chassis] タブを選択します。
- ステップ 3 [Add Tags] をクリックします。  
(注) リストからサーバを選択するまでは、[Add Tags] ボタンは表示されません。
- ステップ 4 ドロップダウンリストから [Tag Name] を選択します。
- ステップ 5 ドロップダウンリストから [Tag Value] を選択します。
- ステップ 6 [+] アイコンをクリックして、新しいタグを作成します。タグの作成については、[Cisco UCS C3260 ラック サーバのタグの管理](#)、(157 ページ) を参照してください。  
(注) また、タグの詳細を編集、削除、表示することもできます。

## ポリシーとプロファイル

Cisco IMC Supervisor には、シャーシ情報を追加できる Cisco UCS C3260 シャーシのポリシーとプロファイルを作成するための新しい [Cisco UCS C3260] オプションとがあります。

本書では、これらの新しいシャーシポリシーはユーザ管理ポリシーと呼び、既存のラックマウントサーバポリシーはコンピューティング ノード ポリシーと呼びます。差別化されたユーザ管理ポリシーとコンピューティング ノード ポリシーの一覧は、[Hardware Policies] テーブルで確認できます。ユーザ管理ポリシーのサーバプラットフォームは [Cisco UCS C3260]、コンピューティング ノード ポリシーは [All C-Series and E-Series except Cisco UCS C3260] と表示されます。

ポリシーとプロファイルのレポートに [Server Platform] という新しい列が追加されており、ポリシーが Cisco UCS C3260 のものかどうかを示されます。シャーシポリシーは、ユーザ管理ポリシーやコンピューティング ノード ポリシーに関係なく [Cisco UCS C3260] と表示されます。他の C シリーズや E シリーズのプラットフォームまたは Cisco UCS C3260 以外のポリシーの場合、[All C-Series and E-Series except Cisco UCS C3260] と表示されます。

Cisco UCS C3260 シャーシプロファイルまたはラックマウントサーバプロファイルを作成できます。コンピューティング ノード ポリシーを選択すると、ポリシーを適用するサーバノードを選択できます。

## ポリシーの適用

作成したポリシーを適用するには、Cisco UCS 3260 ラック サーバとラックマウントサーバのリストから選択します。選択したサーバプラットフォームに基づき、Cisco UCS C3260 シャーシまたはラックマウントサーバを選択できます。ポリシーの作成および適用の詳細については、[ハードウェア ポリシー](#)、(92 ページ) を参照してください。

次のポリシーは、ユーザ管理ポリシーとコンピューティング ノード ポリシーです。

ユーザ管理ポリシー	コンピューティング ノード ポリシー
ユーザ	BIOS
SNMP	Precision Boot Order
LDAP	RAID
NTP	KVM
ネットワーク セキュリティ	vmedia
SSH	VIC
NTP	Serial Over LAN



(注)

- Cisco UCS 3260 ラック サーバの場合、IPMI Over LAN およびネットワーク ポリシーには、BMC と CMC の両方の構成の詳細が混在しています。
- ゾーン分割ポリシーは、Cisco UCS 3260 ラック サーバにのみ適用可能なため、UI の [Cisco UCS C3260] チェック ボックスはオンになっています。
- レガシー ブート順序および Flex Flash のポリシーは、Cisco UCS 3260 ラック サーバには適用できません。

## プロファイルの適用

作成した Cisco UCS C3260 プロファイルを適用するには、Cisco UCS 3260 ラック サーバのリストから選択します。Cisco UCS C3260 シャーシのみ選択でき、Cisco UCS C3260 ポリシーのみプロファイルに追加できます。コンピューティング ノードポリシーの場合は、[Apply Policy To] フィールドを選択して、プロファイル適用時にポリシーを適用する必要があるサーバ ノードを示すことができます。プロファイルの作成および適用の詳細については、[ハードウェア プロファイル](#)、(128 ページ) を参照してください。

## ファームウェアのアップグレード

Cisco IMC Supervisor ファームウェアのアップグレードはサーバレベルで実行できます。ただし、サーバのアップグレード時に、そのサーバに関連付けられているシャーシコンポーネントおよびハードディスクドライブコンポーネントもアップグレードされます。サーバをアップグレードする場合、シャーシとディスクドライブのファームウェアが自動的に更新されます。ファームウェアのアップグレードの詳細については、[ファームウェアのアップグレード](#)、(139 ページ) を参照してください。



(注) 一度に 1 つのサーバノードのみアップグレードできます。

## Cisco UCS C3260 高密度ストレージラック サーバの詳細情報の表示

Cisco UCS C3260 高密度ストレージラック サーバの詳細 (PSU、VIC Adapters、Chassis Summary、SAS Expander など) を表示する場合は、次の手順を実行します。

### はじめる前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

### 手順

- ステップ 1 メニューバーで、[Systems] > [Inventory and Fault Status] を選択します。
- ステップ 2 左側のペインで、[Rack Groups] を展開し、Cisco UCS C3260 高密度ストレージラック サーバを含むラック グループを選択します。
- ステップ 3 右側のペインで、[Chassis] タブを選択します。
- ステップ 4 リストにある Cisco UCS C3260 高密度ストレージラック サーバをダブルクリックして詳細を表示するか、リストにある Cisco UCS C3260 高密度ストレージラック サーバをクリックして [View Details] を選択します。

(注) リストから Cisco UCS C3260 高密度ストレージラック サーバを選択するまでは、[View Details] オプションは表示されません。

Cisco UCS C3260 高密度ストレージラック サーバの次の詳細を表示できます。

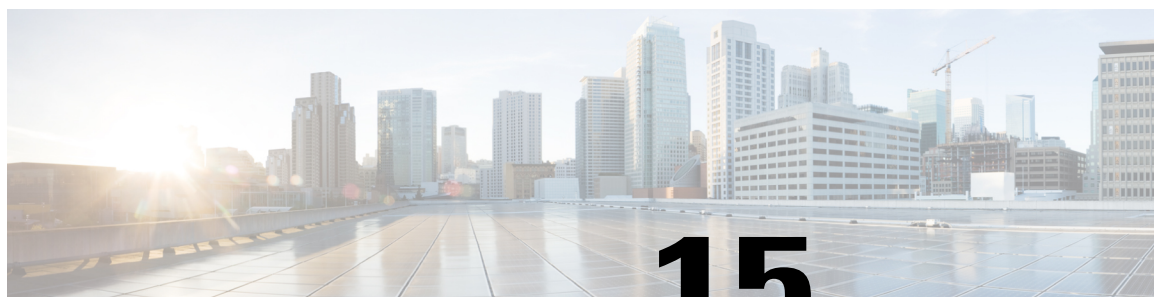
タブ	説明
[PSUs]	サーバで使用されている電源装置の詳細。  (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。

タブ	説明
[VIC Adapters]	サーバで使用されている VIC アダプタの詳細。 リストにある任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] や [VM FEXs] などの情報が表示されます。
[Communication]	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルの情報。
[Remote Presence]	vKVM、Serial over LAN、vMedia の詳細。
[Faults]	サーバで記録された障害の詳細。
[Users]	ユーザの詳細。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[Cisco IMC Log]	サーバの Cisco IMC ログの詳細。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
System Event Log	サーバ ログの詳細。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[Fault History]	サーバで発生した障害の履歴情報。
[Tech Support]	ファイル名、宛先タイプ、アップロードのステータスなどのテクニカルサポート ログ ファイルに関する詳細は、[Tech Support] テーブルに表示されます。 リモート サーバまたはローカルの Cisco IMC Supervisor アプライアンスにテクニカルサポート ログ ファイルをエクスポートするオプションがあります。エクスポートの詳細については、 <a href="#">リモートサーバへのテクニカルサポート データのエクスポート</a> 、(85 ページ) を参照してください。 (注) Cisco UCS C3260 高密度ストレージラック サーバの場合は該当しません。
[Associated Hardware Profiles]	ハードウェア プロファイルに関連付けられているポリシーの詳細。
[Chassis Summary]	CMC 1 ネットワーク、共通、NIC などのプロパティの要約。
[Rack Servers]	ホスト名、IP アドレス、接続ステータスなどのラック サーバの詳細。

タブ	説明
[System IO Controller]	IP アドレス、MAC アドレス、ファームウェア バージョンなどの詳細。
[SAS Expander]	ID、SAS 名、ファームウェア バージョンなどの詳細。
[Zoning]	状態、プレゼンス、所有権、サイズなどの詳細。

**ステップ 5** 右端の [Back] ボタンをクリックして前のウィンドウに戻ります。

---



# 第 15 章

## サポート情報の表示

この章は、次の内容で構成されています。

- [サポート情報, 163 ページ](#)

## サポート情報

Cisco IMC Supervisor サポートはログを表示してダウンロードする基本、高度なシステム情報が表示されます。また、録音したデバッグを記録し、APIのログをダウンロードします。

## サポート情報の表示

Cisco IMC Supervisor のサポート情報を表示するには、次の手順を使用します。

はじめる前に

ポップアップブロッカーが Web ブラウザで無効になっていることを確認します。

手順

**ステップ 1** メニューバーで、[Administration] > [Support Information] を選択します。

**ステップ 2** [Support Information] ウィンドウで、次の情報を表示できます。

表 2: システム情報 (基本)

フィールド	説明
[Support Information] ドロップダウンリスト	基本情報を表示するには、[System Information (Basic)] を選択して [Submit] をクリックします。

表 3: システム情報 (詳細)

フィールド	説明
[Support Information] ドロップダウンリスト	プロセッサ、メモリ、ディスク情報などの詳細情報を表示するには、[System Information (Advanced)] を選択して [Submit] をクリックします。

表 4: View Logs

フィールド	説明
[Support Information] ドロップダウンリスト	[Show log] を選択します。
[Show Log] ドロップダウンリスト	表示するログタイプを選択して、[Show Logs] をクリックします。

表 5: すべてのログのダウンロード

フィールド	説明
[Support Information] ドロップダウンリスト	[Download All Logs] を選択して [Download] をクリックします。

表 6: デバッグログのダウンロード

フィールド	説明
[Support Information] ドロップダウンリスト	<ol style="list-style-type: none"> <li>[Debug Logging] を選択して [Start Debug Logging] をクリックします。</li> <li>停止してログデータをダウンロードするには、[Stop Debug Logging] をクリックして、デバッグのダウンロードリンクをクリックします。</li> </ol>



表 7: API ロギング

フィールド	説明
[Support Information] ドロップダウンリスト	<ol style="list-style-type: none"><li data-bbox="797 386 1520 457">1 [API Logging] を選択して [Start API Logging] をクリックします。</li><li data-bbox="797 478 1520 579">2 停止してログデータをダウンロードするには、[Stop API Logging] をクリックして、API デバッグ ログのダウンロードリンクをクリックします。</li></ol>





# 第 16 章

## 頻繁に実行するタスクおよび手順

この章は、次の内容で構成されています。

- [頻繁に実行する手順, 167 ページ](#)
- [その他の手順, 167 ページ](#)

### 頻繁に実行する手順

この項では、Cisco IMC Supervisor で頻繁に実行する手順にすばやくアクセスできます。参照先は、詳細な手順が説明されている本マニュアルの各項にリンクしています。

手順	参照先
Cisco IMC Supervisor へのログイン方法	<a href="#">Cisco IMC Supervisor の起動, (16 ページ)</a>
ライセンスのアップグレード方法	<a href="#">ライセンスの更新, (17 ページ)</a>
Cisco IMC Supervisor にログインユーザを追加する方法	<a href="#">ユーザアカウントの作成, (45 ページ)</a>
ラック グループの追加方法	<a href="#">ラック グループの追加, (57 ページ)</a>
ラック アカウントの作成方法	<a href="#">ラック アカウントの追加, (58 ページ)</a>

### その他の手順

次の項には、Cisco IMC Supervisor を使用して実行するさまざまな手順が含まれています。

## ダッシュボードビューの有効化

Cisco IMC Supervisor メニューバーのダッシュボードビューを有効にするには、次の手順を実行します。

### 手順

- 
- ステップ 1 アプリケーションにログインしているユーザ名をクリックします。ユーザ名はアプリケーションヘッダーの右端にあります。
  - ステップ 2 [User Information] ウィンドウで [Dashboard] をクリックします。
  - ステップ 3 [Enable Dashboard (in the top level menu)] チェックボックスをオンにしてダッシュボードを有効にします。
  - ステップ 4 [Apply] をクリックし、ウィンドウを閉じます。  
(注) メニューバーに [Dashboard] タブが表示されます。
- 

## ダッシュボードの自動更新の有効化

ダッシュボードに追加したレポートの自動更新を有効にするには、次の手順を実行します。更新率も定義できます。

### 手順

- 
- ステップ 1 メニューバーから [Dashboard] を選択します。
  - ステップ 2 [Dashboard] パネルで、[Automatic Refresh] オプションの横にある [OFF] をクリックします。[Automatic Refresh] オプションが [ON] に変わり、[Interval] スライドバーが表示されます。
  - ステップ 3 [Interval] を使用して、更新率を設定します。  
(注) 更新率は 5 分単位で最大 60 分まで設定できます。
- 

## ダッシュボードへのサマリーレポートの追加

すぐにアクセスできるようにサマリーレポートをダッシュボードに追加するには、次の手順を実行します。



(注) サマリー レポートのみをダッシュボードに追加できます。

#### 手順

- ステップ 1 ダッシュボードに追加するサマリー レポートを参照します。
- ステップ 2 レポート パネルの右上隅にある下向き矢印をクリックします。
- ステップ 3 [Add to Dashboard] をクリックします。  
(注) サマリーレポートがダッシュボードビューに対応している場合にのみ、[Add to Dashboard] オプションが選択可能になります。
- ステップ 4 メニュー バーから [Dashboard] を選択し、レポートがダッシュボードに表示されることを確認します。

## [Favorites] へのメニューまたはタブの追加

[Favorites] メニューにメニュー オプションまたはタブを追加するには、次の手順を実行します。

#### 手順

- ステップ 1 [Favorites] メニューに追加するメニューまたはタブに移動します。
- ステップ 2 [Favorite] をクリックします。  
(注) [Favorite] ボタンは、これに対応しているメニューまたはタブのみに表示されません。
- ステップ 3 [Favorite Report] ダイアログボックスで、[Menu Label] フィールドを編集できます。
- ステップ 4 [Save] をクリックします。
- ステップ 5 メニュー バーで [Favorites] を選択し、新しいメニューが表示されることを確認します。

## レポート テーブル ビューのカスタマイズ

レポート テーブルのフィールドを追加または削除するには、次の手順を実行します。

#### はじめる前に

テーブルのカスタマイズに対応しているウィンドウでは、ページの右端に [Customize Table View] アイコンが表示されます。

## 手順

---

- ステップ 1** ページの右端で [Customize Table View] アイコンを見つけてクリックします。
- ステップ 2** [Customize Report Table] ダイアログボックスでは、次の操作が可能です。
- テーブルレポートのフィールドを表示するには、そのフィールドの横のチェックボックスをオンにします。
  - テーブルレポートからフィールドを削除するには、そのフィールドの横のチェックボックスをオフにします。
  - デフォルトのテーブル ビューにリセットするには、[Reset to Default] をクリックします。
- ステップ 3** [Save] をクリックします。
- 

## レポートのフィルタリング

ユーザ定義の条件に基づいてデータをフィルタリングするには、次の手順を実行します。

### はじめる前に

データのフィルタリングに対応しているウィンドウでは、ページの右端に [Add Advanced Filter] アイコンが表示されます。

## 手順

---

- ステップ 1** ページの右端で [Add Advanced Filter] アイコンを見つけてクリックします。アイコンをクリックするたびに、レポートテーブルの上部にフィルタ条件が追加されます。
- ステップ 2** [Match Condition] ドロップダウンリストで、必要に応じて [Match All Conditions] または [Match Any Condition] を選択します。
- ステップ 3** [Search in Column] ドロップダウンリストで、データをフィルタリングするためのフィールドを選択します。
- ステップ 4** [Text] フィールドに、データをフィルタリングするための値を入力します。
- ステップ 5** 複数のフィルタ条件がある場合は、すべての条件に対して [ステップ 3](#)、[\(170 ページ\)](#) と [ステップ 4](#)、[\(170 ページ\)](#) を繰り返します。
- ステップ 6** [Search] をクリックします。
-

## レポートのエクスポート

PDF、CSV、XLS 形式でレポート データをエクスポートするには、次の手順を実行します。

### はじめる前に

レポート データのエクスポートに対応しているウィンドウでは、ページの右端に [Export Report] アイコンが表示されます。

### 手順

---

**ステップ 1** ページの右端で [Export Report] アイコンを見つけてクリックします。

**ステップ 2** [Export Report] ダイアログボックスで、次の手順を実行します。

- 1 [Select Report Format] ドロップダウン リストから、[PDF]、[CSV]、または [XLS] を選択します。
- 2 [Generate Report] をクリックします。
- 3 レポートが生成されたら、[Download] をクリックします。

選択した形式のレポートが新しいウィンドウに生成されます。

**ステップ 3** [Export Report] ダイアログボックスで [Close] をクリックします。

---

