Cisco IMC Supervisor ラックマウント サーバ管理ガイド、リリース 1.0

初版：2014 年 11 月 24 日

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

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

© 2014 Cisco Systems, Inc. All rights reserved.

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

概要 1

Cisco IMC Supervisor について 1

ライセンスについて 2

製品アクセス キーの契約履行 2

Cisco IMC Supervisor ユーザ インターフェイスの共通用語 3

ラック グループ 3

ラック アカウント 3

使用する前に 5

Cisco IMC Supervisor の起動 5

ライセンスの更新 6

ラック グループの追加 6

ラック アカウントの追加 7

[Systems] メニューを使用したサーバの管理 9

ラック グループのインベントリおよび障害のステータス 9

[Inventory and Fault Status] タブでのサーバ タスク 10

ラックマウント サーバの詳細の表示 10

ラックマウント サーバ障害の詳細の表示 12

ラックマウント サーバの電源オン/オフ 13

ラックマウント サーバのシャットダウン 13

ラックマウント サーバのハード リセットの実行 14

ラックマウント サーバの電源再投入の実行 14

ラックマウント サーバの KVM コンソールの起動 15
ラックマウント サーバの GUI の起動 15
ラックマウント サーバのロケータ LED の設定 16
ラックマウント サーバのラベルの設定 16
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 17
SEL のクリア 18
[Physical Accounts] メニュー 19
物理サーバの管理 19
ラック グループの管理 19
ラック グループの追加 19
ラック グループの編集 19
ラック グループの削除 20
ラック アカウントの管理 21
ラック アカウントの追加 21
ラック アカウントの編集 21
アカウント接続のテスト 22
ラック アカウントの削除 23
サーバ検出の管理 23
サーバの検出およびインポート 23
自動検出プロファイルの設定 24
自動検出の実行 26
サーバのインポート 26
自動検出プロファイルの削除 27
自動検出リストのクリア 28
ファームウェア アップグレード 29
ファームウェアのアップグレード 29
ファームウェア アップグレード用プロファイルの設定 29
ファームウェアのアップグレード 31
ファームウェアの削除 31
ファームウェア アップグレード用に作成されたプロファイルの削除 32
ファームウェア ステータス メッセージのクリア 33
[Policies] メニュー 35

[Policies] メニューのオプション 35
Credential Policies 35
Tag Library 36
[Credential Policies] でのポリシー タスク 36
クレデンシャル ポリシーの作成 36
クレデンシャル ポリシーの編集 37
クレデンシャル ポリシーの複製 38
クレデンシャル ポリシーの削除 39
クレデンシャル ポリシーの詳細の表示 39
[Tag Library] でのタグ付けタスク 40
タグ ライブラリの作成 40
タグ ライブラリの複製 41
タグ ライブラリの編集 43
タグ ライブラリの削除 45
タグの詳細の表示 45
タグ関連付けの詳細の表示 46
Cisco IMC Supervisor 管理機能 47
[License] メニュー 47
[System] メニュー 48
[Users] メニュー 49
[Integration] メニュー 49
User Interface Settings 50
サポート情報 50
ライセンス情報の管理 51
アップグレード ライセンスの適用 51
ライセンス監査の実行 51
システム情報の管理 52
[Mail Setup] の設定 52
システム タスクの管理 53
タスクの実行 54
電子メール アラートの設定 54
ユーザ ロールの管理 55
ユーザ ロールの追加 55

ユーザ ロールの編集 56
ユーザ ロールの複製 56
ユーザ ロールの削除 57
ユーザの管理 58
ログイン ユーザの管理 58
ログイン ユーザの追加 58
ログイン ユーザの編集 59
ログイン ユーザの削除 60
ユーザ パスワードの変更 60
ブランディング ページの管理 61
新しいログイン ブランディングの追加 61
ブランディング ページの編集 62
ブランディング ページの複製 63
認証設定の管理 63
LDAP 統合 64
LDAP 統合の規則と制限事項 64
LDAP サーバのサマリー情報の表示 65
LDAP サーバの接続のテスト 66
LDAP サーバの詳細の変更 66
LDAP サーバ情報の削除 67
ユーザ パスワード ポリシーの管理 68
統合の管理 68
[CMDB Integration Setup] の設定 68
監査ログの表示 69
[User Interface Settings] の設定 70
サポート情報の表示 71
頻繁に実行するタスクおよび手順 75
頻繁に実行する手順 75
その他の手順 76
ダッシュボードの自動更新の有効化 76
ダッシュボードへのサマリー レポートの追加 76
[Favorites] へのメニューまたはタブの追加 77

レポート テーブル ビューのカスタマイズ 77
レポートのフィルタリング 78
レポートのエクスポート 78

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 使用する 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	用途
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。

テキストのタイプ	用途
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（*italic*）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（**bold**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）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。

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。

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

ワンポイント アドバイス 「時間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 安全上の重要事項

「危険」の意味です。 人身事故を予防するための注意事項が記述されています。 機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。 警告の各国語版については、各警告文の末尾に提示されている番号をもとに、この機器に付属している各国語で記述された安全上の警告を参照してください。

これらの注意事項を保存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

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，1 ページ
- ライセンスについて，2 ページ
- 製品アクセス キーの契約履行，2 ページ
- Cisco IMC Supervisor ユーザ インターフェイスの共通用語，3 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 を使用してラック マウント サーバに対して次のタスクを実行できます。

- サーバの論理グループ化およびグループごとのサマリー表示のサポート
- サーバ インベントリの収集
- サーバおよび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管理
- 電源制御、LED 制御、ログの収集、KVM の起動、CIMC UI の起動および電子メール アラートなど、スタンドアロン サーバのアクションの管理
- アクセスを制限するためのロールベース アクセス コントロール（RBAC）

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。

ライセンスの取得およびインストールのプロセスは両方のライセンスに共通です。

Cisco IMC Supervisor を使用するには、次の手順に従ってライセンスを取得する必要があります。

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, （2 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, （6 ページ）の手順に従って、Cisco IMC Supervisor で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。

製品アクセス キーの契約履行

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。

フィールド	説明
Street Address	組織の番地。
City/Town	市区町村名。
State/Province	州/都道府県。
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 スタックを表すことができます。 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） Cisco IMC Supervisor にはすでにデフォルト グループが含まれています。 デフォルト グループは削除または変更できません。 要件に従って、新しいラック アカウントをデフォルト グループに追加するか、または新しいラック グループを作成することができます。

ラック アカウント

ラック アカウントとは、Cisco IMC Supervisor に追加されたスタンドアロン 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。

第 2 章

使用する前に

この章は、次の内容で構成されています。

- Cisco IMC Supervisor の起動，5 ページ
- ライセンスの更新，6 ページ
- ラック グループの追加，6 ページ
- ラック アカウントの追加，7 ページ

Cisco IMC Supervisor の起動

Cisco IMC Supervisor にログインするには、次の手順を実行します。

はじめる前に

- Cisco IMC Supervisor が正常にインストールされています。
- Cisco IMC Supervisor インストール中に IP アドレスが設定されています。

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

ライセンスの更新

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。

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。 ライセンスの更新については、ライセンスの更新, （6 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 [Create] 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	（オプション）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

Cisco IMC Supervisor のラック グループのいずれかにラックマウント サーバを追加できます。 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 用にライセンスが更新されていることを確認します。 ライセンスの更新については、ライセンスの更新, （6 ページ）を参照してください。
- ラック グループはすでに作成済みです。

（注） 新しいラック グループを作成しなくても、[Default Group] にラック アカウントを追加できます。

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 [追加]（+）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
[アカウント名] 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。
[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。
[Rack Group] ドロップダウン リスト	リストからラック グループを選択します。
[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。

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，（22 ページ）を参照してください。

第 3 章

[Systems] メニューを使用したサーバの管理

この章は、次の内容で構成されています。

- ラック グループのインベントリおよび障害のステータス，9 ページ
- [Physical Accounts] メニュー，19 ページ

ラック グループのインベントリおよび障害のステータス

[Systems] メニューには、[Inventory and Fault Status] および [Physical Accounts] メニュー オプションが含まれます。 [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。 リストが折りたたまれている場合は、[Rack Groups] の横の下向き矢印をクリックしてビューを展開します。 デフォルトのラック グループおよびユーザが定義したすべてのラック グループが表示されます。 このオプションを使用して、すべての C シリーズおよび E シリーズ サーバを管理およびモニタできます。

（注） 初回ログイン時に使用できるラック グループは、デフォルト グループのみです。 ラック グループの追加については、ラック グループの追加，（6 ページ）を参照してください。

左側のペインで [Rack Groups] 見出しが選択されている場合、右側のペインでは次のタブを使用できます。

タブ	説明
Summary	すばやく表示できるように、サマリー レポートを [Summary] ページに追加できます。 サマリー レポートの追加については、ダッシュボードへのサマリー レポートの追加，（76 ページ）を参照してください。
Rack Servers	[Rack Servers] タブには、すべてのラック グループに追加されたラックマウント サーバの詳細が表示されます。

タブ	説明
Faults	[Faults] タブには、Cisco IMC Supervisor で記録されたすべての障害の詳細が表示されます。
More Reports	[More Reports] タブには、障害、サーバ ヘルス、ファームウェア バージョン、サーバ モデル、電源状態に関する追加レポートが円グラフの形式で表示されます。

いずれかのラック グループ（デフォルト グループを含む）が左側のペインで選択されている場合、右側のペインで次のタブを使用できます。

タブ	説明
Summary	すばやく表示できるように、選択したグループのサマリー レポートを [Summary] ページに追加できます。 サマリー レポートの追加については、ダッシュボードへのサマリー レポートの追加, （76 ページ）を参照してください。
Rack Servers	[Rack Servers] タブには、選択したラック グループに追加されたラックマウント サーバの詳細が表示されます。
Faults	[Faults] タブには、ラックマウント サーバの選択したラック グループで記録されたすべての障害の詳細が表示されます。
More Reports	[More Reports] タブには、障害、サーバ ヘルス、ファームウェア バージョン、サーバ モデル、電源状態に関する追加レポートが円グラフの形式で表示されます。

[Inventory and Fault Status] タブでのサーバ タスク

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
Summary	ラック アカウントの概要が表示されます。
CPUs	サーバで使用されている CPU の詳細が表示されます。
Memory	サーバで使用されているメモリの詳細が表示されます。
PSUs	サーバで使用されている電源装置の詳細が表示されます。
PCI Adapters	サーバで使用されている PCI アダプタの詳細が表示されます。
VIC Adapters	サーバで使用されている VIC アダプタの詳細が表示されます。
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 アダプタの詳細が表示されます。
Faults	サーバで記録された障害の詳細が表示されます。
Cisco IMC Log	サーバの Cisco IMC ログの詳細が表示されます。
System Event Log	サーバ ログの詳細が表示されます。
TPM	TPM インベントリに関する情報が表示されます。
Fault History	サーバで発生した障害の履歴情報が表示されます。

タブ	説明
Tech Support	次のプロトコルのいずれかを使用して、リモート サーバにテクニカル サポート ログ ファイルをエクスポートするためのオプションが表示されます。 • FTP • TFTP • SFTP • SCP （注） 現在、ローカル システムへのテクニカル サポート ログ ファイルのダウンロードはサポートされていません。

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移動します。

ラックマウント サーバ障害の詳細の表示

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、[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 右端の [Back] ボタンをクリックして前のウィンドウに移動します。

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 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。
ステップ 5 [Power On] または [Power OFF] 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 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。

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。

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] タブを選択します。
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。

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

ラックマウント サーバのハード リセットを実行する場合は、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。
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 サーバに電源を再投入する場合は、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。

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

ラックマウント サーバの KVM コンソールを起動する場合は、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） リストからサーバを選択するまでは、[KVM Console] ボタンは表示されません。
ステップ 6 [Submit] をクリックします。
Cisco IMC Supervisor によって *kvm.jlp* 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.jlp* 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。
必要な Java ランタイム環境（JRE）がインストールされていない場合は、ダイアログボックスの [More Info] をクリックし、画面の手順に従って JRE をダウンロードしてインストールします。

ラックマウント サーバの GUI の起動

ラックマウント サーバの GUI を起動する場合は、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

ラックマウント サーバのロケータ LED を設定する場合は、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

ラックマウント サーバのラベルを設定する場合は、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。

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

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 [Tech Support] タブをクリックします。
ステップ 6 [Upload Logs] をクリックします。
ステップ 7 [Upload Technical Logs] 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
[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。 • TFTP • FTP • SFTP • SCP

名前	説明
[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のあるサーバの 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のあるユーザ名。 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。

SEL のクリア

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。

[Physical Accounts] メニュー

[Physical Accounts] メニューには次のタブが表示されます。

タブ	説明
Rack Groups	このタブには、Cisco IMC Supervisor のすべてのラック グループが表示されます。
Rack Accounts	このタブには、Cisco IMC Supervisor のすべてのラック アカウントが表示されます。 このタブを使用して、ラック アカウントを作成、編集、削除、およびテストすることもできます。
Discovered Devices	このタブには、設定されたサブネット内のすべてのデバイスが表示されます。 また、このタブでプロファイルを設定および削除できます。
Firmware Upgrades	このタブでは、ファームウェア アップグレード用プロファイルを作成し、デバイスをアップグレードすることができます。

物理サーバの管理

ラック グループの管理

ラック グループの追加

ラック グループの作成については、ラック グループの追加, （6 ページ）を参照してください。

ラック グループの編集

ラック グループを編集する場合は、次の手順を実行します。

はじめる前に

ラック グループは、[Rack Groups] にすでに作成されています。

（注） デフォルト ラック グループは編集できません。

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 グループのリストから、編集するグループを選択します。

ステップ 3 [Modify] をクリックします。

（注） リストからラック グループを選択するまでは、[Modify] ボタンは表示されません。

ステップ 4 [Modify 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
[New Group Name] フィールド	ラック グループの記述名。
[New Description] フィールド	（オプション）ラック グループの説明。

ステップ 5 [Modify] 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。

ラック グループの削除

ラック グループを削除する場合は、次の手順を実行します。

はじめる前に

ラック グループは、[Rack Groups] にすでに作成されています。

（注） デフォルト ラック グループは削除できません。

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 グループのリストから、削除するグループを選択します。

ステップ 3 [Delete] をクリックします。

（注） リストからラック グループを選択するまでは、[Delete] ボタンは表示されません。

ステップ 4 （任意） 削除するラック グループに関連付けられているラック アカウントを削除する場合は、[Delete rack accounts within rack group (rack group name)] チェックボックスをオンにします。

（注） [Delete rack accounts within rack group (rack group name)] チェックボックスがオフになっている場合、関連付けられているラック アカウントは、[Default Group] に移動されます。

ステップ 5 [Delete] 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。

ラック アカウントの管理

ラック アカウントの追加

ラック アカウントの作成については、ラック アカウントの追加, （7 ページ）を参照してください。

ラック アカウントの編集

ラック アカウントを編集する場合は、次の手順を実行します。

はじめる前に

ラック アカウントは、[Rack Accounts] 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 アカウントのリストから、編集するアカウントを選択します。

ステップ 4 [Modify] をクリックします。

（注） リストからラック アカウントを選択するまでは、[Modify] ボタンは表示されません。

ステップ 5 [Modify 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
[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	

フィールド	説明
[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。
[Rack Group] ドロップダウン リスト	リストからラック グループを選択します。
[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 6 [Modify] をクリックします。

ステップ 7 [OK] をクリックします。

アカウント接続のテスト

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。

はじめる前に

ラック アカウントは、[Rack Accounts] 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、[Administration] > [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） リストからラック アカウントを選択するまでは、[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。

ラック アカウントの削除

ラック アカウントを削除する場合は、次の手順を実行します。

はじめる前に

ラック アカウントは、[Rack Accounts] 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から、削除するアカウントを選択します。
ステップ 4 [Delete] をクリックします。
ステップ 5 [Delete Rack Server Accounts] ダイアログボックスで、[Select] をクリックし、削除するラック アカウントのチェックボックスをオンにします。
ステップ 6 [Select] をクリックします。
ステップ 7 [Submit] をクリックします。
ステップ 8 確認ダイアログボックスで、[OK] をクリックします。

サーバ検出の管理

サーバの検出およびインポート

自動検出を実行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。

手順

	コマンドまたはアクション	目的
ステップ 1	検出プロファイルを設定します。	自動検出プロファイルの設定, （24 ページ）を参照してください。
ステップ 2	サーバを検出します。	自動検出の実行, （26 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 3	サーバをインポートします。	サーバのインポート, （26 ページ）を参照してください。
ステップ 4	検出プロファイルを削除します。	（任意）自動検出プロファイルの削除, （27 ページ）を参照してください。
ステップ 5	自動検出リストからサーバをクリアします。	（任意）自動検出リストのクリア, （28 ページ）を参照してください。

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、[Administration] > [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 [Configure] をクリックします。

ステップ 4 [Discovery Configuration Criteria] ダイアログボックスで、新しいプロファイルを作成するか、既存のプロファイルを編集することができます。
新しいプロファイルを作成するには、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 [<New>] を選択します。
[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。
[IP Address Range] を選択した場合	
[Starting IP] フィールド	有効な IP アドレス

フィールド	説明
[Ending IP] フィールド	有効な IP アドレス
[Subnet Mask Range] を選択した場合	
[Network Address] フィールド	有効な IP アドレス
[Subnet Mask] ドロップダウン リスト	ドロップダウン リストから値を選択します。
[IP Address CSV File] を選択した場合	
[アップロードするファイルの選択] フィールド	[Browse] をクリックし、IP アドレスが含まれている .csv ファイルに移動します。
[IP Address List] を選択した場合	
[IP Addresses] フィールド	複数の IP アドレスをカンマで区切って入力します。
[Use Credential Policy] チェックボックス	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	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、クレデンシャル ポリシーの作成, （36 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。

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。

自動検出の実行

自動検出を実行する場合は、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、[Administration] > [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、[Select Profile] ドロップダウン リストからプロファイルを選択します。
ステップ 5 [Submit] をクリックします。
ステップ 6 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。

重要 アカウントの追加、変更、インポートなどの複数のアカウント関連タスクを、Cisco IMC Supervisor で同時に実行することはできません。 1 つのタスクが完了するまで待って、別のタスクを開始することを推奨します。 たとえば、検出されたデバイスをラック グループにインポート中である場合、別のラック グループまたはラック アカウントを編集する前にこのタスクを完了させることを推奨します。 進行中のアカウント タスクの状態を確認するには、[Administration] > [System] > [System Tasks] > [Rack Server Tasks] を選択し、[Rack Server OnDemand Inventory] タスクが [In Progress] であるかどうかを判別します。

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手順を実行し、[Select] ボタンをクリックします。

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） サーバについては、[Account Exists] カラムに [Yes] のマークが付いている場合、現在このアカウントが Cisco IMC Supervisor によって管理されていることを意味します。 エラーを防ぐために、[No] とマークされているアカウントを選択してください。
[Select Rack Group] ドロップダウン リスト	ラック 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 確認ダイアログボックスで、[OK] をクリックします。

自動検出プロファイルの削除

自動検出プロファイルを削除する場合は、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、[Administration] > [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 [Delete Profile] をクリックします。
ステップ 4 [Delete Profile] ダイアログボックスで、[Select Profile] ドロップダウン リストからプロファイルを選択します。
ステップ 5 [Submit] をクリックします。
ステップ 6 確認ダイアログボックスで、[OK] をクリックします。

自動検出リストのクリア

1 つのサーバまたはすべてのサーバを自動検出リストから削除する場合は、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。
- 自動検出をすでに実行済みです。

手順

ステップ 1 メニュー バーで、[Administration] > [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 [Clear] をクリックします。
ステップ 4 [Clear Devices] ダイアログボックスで、[Select] ボタンをクリックします。
ステップ 5 [Select] ダイアログボックスで、削除するサーバのチェックボックスをオンにします。
（注） すべてのサーバを選択するには、一番上のチェックボックスをオンにします。
ステップ 6 [Select] をクリックします。
ステップ 7 [Clear 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 確認ダイアログボックスで、[OK] をクリックします。

ファームウェア アップグレード

ファームウェアのアップグレード

ファームウェアをアップグレードする場合は、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	ファームウェア アップグレード用プロファイルを設定します。	ファームウェア アップグレード用プロファイルの設定, （29 ページ）を参照してください。
ステップ 2	ファームウェアのアップグレード。	ファームウェアのアップグレード, （31 ページ）を参照してください。
ステップ 3	ファームウェア イメージの削除。	（任意） ファームウェアの削除, （31 ページ）を参照してください。
ステップ 4	ファームウェア アップグレード用プロファイルを削除します。	（任意） ファームウェア アップグレード用に作成されたプロファイルの削除, （32 ページ）を参照してください。

ファームウェア アップグレード用プロファイルの設定

ファームウェア アップグレード用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 [Firmware Upgrades] タブをクリックします。

ステップ 3 [Configure Profile] をクリックします。

ステップ 4 [Download Firmware] ダイアログボックスで、新しいプロファイルを作成するか、既存のプロファイルを編集することができます。
新しいプロファイルを作成するには、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 [<New>] を選択します。
[Profile Name] フィールド	プロファイルの記述名。
[Download Option] 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。 • [Local HTTP Server]：.iso イメージはローカル Cisco IMC Supervisor に保存されます。 • [Network Path]：.iso イメージはネットワークに保存されます。
[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。
[Enable Proxy Configuration] チェックボックス	（オプション）このチェックボックスをオンにしてプロキシ設定を有効にし、以下を実行します。 • [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。 • [Port] フィールド：プロキシ設定用のポートを入力します。
[Enable Proxy Authentication] チェックボックス	（オプション）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にし、以下を実行します。 • [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。 • [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。
[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。
[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。

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。

ファームウェアのアップグレード

ファームウェアをアップグレードする場合は次の手順を実行します。

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。

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 [Firmware Upgrades] タブをクリックします。

ステップ 3 [Upgrade Image] をクリックします。

ステップ 4 [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。
Select Server	[Select Server] をクリックします。 リストからサーバを選択して [Select] 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 確認ダイアログボックスで、[OK] をクリックします。

ファームウェアの削除

ファームウェアを削除する場合は、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 [Firmware Upgrades] タブをクリックします。
ステップ 3 [Delete Image] をクリックします。
ステップ 4 [Delete Firmware Image] 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
[Delete 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。

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。

ファームウェア アップグレード用に作成されたプロファイルの削除

ファームウェア アップグレード用に作成されたプロファイルを削除する場合は、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 [Firmware Upgrades] タブをクリックします。
ステップ 3 [Delete Profile] をクリックします。
ステップ 4 [Delete Profile] 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。

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。

ファームウェア ステータス メッセージのクリア

すべてのファームウェア関連ステータス メッセージを Cisco IMC Supervisor インターフェイスからクリアするには、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] > [Physical Accounts] 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 [Clear] をクリックします。
ステップ 4 [Clear Firmware Status Messages] ダイアログボックスで、[Submit] をクリックします。
ステップ 5 [OK] をクリックします。

第 4 章

[Policies] メニュー

この章は、次の内容で構成されています。

- [Policies] メニューのオプション，35 ページ
- [Credential Policies] でのポリシー タスク，36 ページ
- [Tag Library] でのタグ付けタスク，40 ページ

[Policies] メニューのオプション

[Policies]ページには、サブメニューオプションに応じて詳細が表示されます。 次のサブメニューオプションがあります。

- Credential Policies
- Tag Library

Credential Policies

[Credential Policies] メニューの唯一のタブには、次の詳細が表示されます。

フィールド	説明
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。

Tag Library

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。

[Credential Policies] でのポリシー タスク

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] > [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。

フィールド	説明
[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。

クレデンシャル ポリシーの編集

クレデンシャル ポリシーを編集する場合は、次の手順を実行します。

はじめる前に

ポリシーは、[Credential Policies] 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、[Policies] > [Credential Policies] を選択します。

ステップ 2 ポリシーのリストから、編集するポリシーを選択します。

ステップ 3 [Edit] をクリックします。

（注） リストからポリシーを選択するまでは、[Edit] ボタンは表示されません。

ステップ 4 [Modify Credential Policy] ダイアログボックスで、次のフィールドを編集します。

フィールド	説明
[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。

フィールド	説明
[Port] フィールド	ポリシーのポート番号を入力します。

（注） ポリシーの名前は変更できません。

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。

クレデンシャル ポリシーの複製

別のポリシーに基づいて新しいクレデンシャル ポリシーを作成する場合は、次の手順を実行します。

はじめる前に

ポリシーは、[Credential Policies] 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、[Policies] > [Credential Policies] を選択します。

ステップ 2 ポリシーのリストから、複製するポリシーを選択します。

ステップ 3 [Clone] をクリックします。

（注） リストからポリシーを選択するまでは、[Clone] ボタンは表示されません。

ステップ 4 [Clone 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。

フィールド	説明
[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 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。

クレデンシャル ポリシーの削除

クレデンシャル ポリシーを削除する場合は、次の手順を実行します。

はじめる前に

ポリシーは、[Credential Policies] 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、[Policies] > [Credential Policies] を選択します。

ステップ 2 ポリシーのリストから、削除するポリシーを選択します。

ステップ 3 [Delete] をクリックします。

（注） リストからポリシーを選択するまでは、[Delete] ボタンは表示されません。

ステップ 4 [Delete Credential Policy] ダイアログボックスで、[Delete] 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。

クレデンシャル ポリシーの詳細の表示

クレデンシャル ポリシー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

ポリシーは、[Credential Policies] 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、[Policies] > [Credential Policies] を選択します。
ステップ 2 ポリシーのリストから、表示するポリシーを選択します。
ステップ 3 [View] をクリックします。
（注） リストからポリシーを選択するまでは、[View] ボタンは表示されません。
ステップ 4 [Credential Policy Details] ダイアログボックスに詳細が表示されます。
ステップ 5 [Close] をクリックして前の画面に戻ります。

[Tag Library] でのタグ付けタスク

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。

はじめる前に

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] 画面で、次の手順を実行します。

名前	説明
[Taggable Entities] フィールド	タグを適用する必要があるエンティティを選択します。 エンティティを追加するには、以下を実行します。 **1** [+] アイコンをクリックします。 **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。 • Physical_Compute • Administration **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。 **4** [Submit] をクリックします。 （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。

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。

タグ ライブラリの複製

別のタグ ライブラリに基づいて新しいタグ ライブラリを作成する場合は、次の手順を実行します。

はじめる前に

タグ ライブラリは、[Tag Library] 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、[Policies] > [Tag Library] を選択します。

ステップ 2 タグ ライブラリのリストから、複製するタグ ライブラリを選択します。

ステップ 3 [Clone] をクリックします。

（注） リストからタグ ライブラリを選択するまでは、[Clone] ボタンは表示されません。

ステップ 4 [Clone 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 5 [Next] をクリックします。

ステップ 6 [Applicability Rules] 画面で、次の手順を実行します。

名前	説明
[Taggable Entities] フィールド	タグを適用する必要があるエンティティを選択します。 エンティティを追加するには、以下を実行します。 **1** [+] アイコンをクリックします。 **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。 • Physical_Compute • Administration **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。 **4** [Submit] をクリックします。 （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。

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。
ステップ 8 [Submit] をクリックします。
ステップ 9 [OK] をクリックします。

タグ ライブラリの編集

タグ ライブラリを編集する場合は、次の手順を実行します。

はじめる前に

タグ ライブラリは、[Tag Library] 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、[Policies] > [Tag Library] を選択します。
ステップ 2 タグ ライブラリのリストから、編集するタグ ライブラリを選択します。
ステップ 3 [Edit] をクリックします。

リストからタグ ライブラリを選択するまでは、[Edit] ボタンは表示されません。

ステップ 4 [Edit 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 5 [Next] をクリックします。

ステップ 6 [Applicability Rules] 画面で、次の手順を実行します。

名前	説明
[Taggable Entities] フィールド	タグを適用する必要があるエンティティを選択します。 エンティティを追加するには、以下を実行します。 **1** [+] アイコンをクリックします。 **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。 • Physical_Compute • Administration **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。 **4** [Submit] をクリックします。 （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。

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。

ステップ 8 [Submit] をクリックします。

ステップ 9 [OK] をクリックします。

タグ ライブラリの削除

タグ ライブラリを削除する場合は、次の手順を実行します。

はじめる前に

タグ ライブラリは、[Tag Library] 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、[Policies] > [Tag Library] を選択します。
ステップ 2 タグ ライブラリのリストから、削除するタグ ライブラリを選択します。
ステップ 3 [Delete] をクリックします。
（注） リストからタグ ライブラリを選択するまでは、[Delete] ボタンは表示されません。
ステップ 4 [Tag] ダイアログボックスで、[Delete] 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。

タグの詳細の表示

タグ ライブラリ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

- タグ ライブラリは、[Tag Library] 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、[Policies] > [Tag Library] を選択します。
ステップ 2 タグ ライブラリのリストから、表示するタグ ライブラリを選択します。
ステップ 3 [View] をクリックします。
（注） リストからタグ ライブラリを選択するまでは、[View] ボタンは表示されません。
ステップ 4 [Tag Details] ダイアログボックスに詳細が表示されます。
ステップ 5 [Close] をクリックして前の画面に戻ります。

タグ関連付けの詳細の表示

タグ ライブラリの関連付け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

タグ ライブラリは、すでに [Tag Library] に作成され、エンティティに関連付けられています。

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 タグ ライブラリのリストから、表示するタグ ライブラリを選択します。

ステップ 3 リストのタグライブラリをダブルクリックする、またはリストのタグライブラリをクリックして [View Details] をクリックします。

（注） リストからタグ ライブラリを選択するまでは、[View Details] ボタンは表示されません。

[Tag Association] ページに次の詳細が表示されます。

フィールド	説明
Tag Name	タグの記述名。
Associated Resource Entity	エンティティの値。
Resource Entity Type	エンティティのリソース タイプ。
Tag Value	タグの値。

ステップ 4 [Close] をクリックして前の画面に戻ります。

第 5 章

Cisco IMC Supervisor 管理機能

この章は、次の内容で構成されています。

- [License] メニュー，47 ページ
- [System] メニュー，48 ページ
- [Users] メニュー，49 ページ
- [Integration] メニュー，49 ページ
- User Interface Settings，50 ページ
- サポート情報，50 ページ
- ライセンス情報の管理，51 ページ
- システム情報の管理，52 ページ
- ユーザの管理，58 ページ
- 統合の管理，68 ページ
- [User Interface Settings] の設定，70 ページ
- サポート情報の表示，71 ページ

[License] メニュー

[License] メニューには次のタブが表示されます。

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更新およびアップグレードすることもできます。

タブ	説明
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。

[System] メニュー

[System] メニューには次のタブが表示されます。

タブ	説明
System Information	基本システム情報には、バージョン、稼動時間、サービス ステータス、システム ライセンス ステータス、使用状況、計算アカウント ステータス、計算サーバ ステータス、ストレージ アカウント ステータス、システム カタログ、およびネットワーク デバイス ステータスが含まれます。
Mail Setup	このタブを使用して SMTP を設定できます。
System Tasks	このタブにはすべてのシステム タスクが表示されます。 このタブを使用してシステム タスクを管理できます。
User Roles	このタブには、すべての Cisco IMC Supervisor ユーザとそのロールが表示されます。 このタブを使用してユーザを管理できます。 （注） これは、ログイン ユーザではありません。 すべての権限を持つ管理者または定義された権限を持つエンド ユーザとして定義されたユーザを指します。 ログイン ユーザは、これらのユーザ ロールのいずれかに基づいて設定できます。
Email Alert Rules	システムからの電子メール アラートのルールを設定する場合にこのタブを使用します。 現在、電子メール アラートを有効にできるのは重大な障害に対してのみです。

[Users] メニュー

[Users] メニューには次のタブが表示されます。

タブ	説明
Login Users	このタブには、Cisco IMC Supervisor にログインできるすべてのユーザが表示されます。 このタブを使用して新しいユーザを作成することもできます。
Currently Online Users	このタブには、現在 Cisco IMC Supervisor にログインしているすべてのユーザが表示されます。
Login Page Branding	このタブには、Cisco IMC Supervisor のカスタマイズされたログイン ページが表示されます。 このタブを使用して、ドメインとロゴを含む新しいログイン ページを作成することもできます。
Authentication Preferences	このタブを使用して、認証設定を [Local Authentication]、[Local first]、[LDAP first]、または [VeriSign Identity Protection] として設定できます。
LDAP Integration	このタブを使用して、LDAP設定の表示と設定操作を実行できます。
Password Policy	このタブを使用してユーザのパスワード ポリシーを変更できます。

[Integration] メニュー

[Integration] メニューには次のタブが表示されます。

タブ	説明
CMDB Integration Setup	このタブを使用して FTP を設定できます。
Change Records	このタブには、Cisco IMC Supervisor で行われた変更のタイムスタンプが表示されます。

User Interface Settings

[User Interface Settings] メニューには次のフィールドが表示されます。

フィールド	説明
[Product Name] フィールド	ヘッダーバーの左端のタイトルテキストを変更するには、このフィールドを設定します。
[Product Name 2nd Line] フィールド	ヘッダー バーの左端にあるタイトルの下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。
[Enable About Dialog] チェックボックス	ヘッダーバーの [About] を有効または無効にするには、このオプションを設定します。
管理者ポータル	
[Custom Link 1 Lable] 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。
[カスタムリンク1の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 Lable] 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。
[カスタムリンク2の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。
エンド ユーザ ポータル	
[Custom Link 1 Lable] 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。
[カスタムリンク1の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 Lable] 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。
[カスタムリンク2の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。

サポート情報

[Support Information] メニューを使用して、Cisco IMC Supervisor で表示するサポート情報のタイプを設定できます。

ライセンス情報の管理

アップグレード ライセンスの適用

Cisco IMC Supervisor ライセンスをアップグレードする必要があります。

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] タブをクリックします。

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、次の手順を実行します。

フィールド	説明
[Select File to Upload] フィールド	[Browse] をクリックし、ライセンス ファイルを見つけて選択します。 ファイルを選択したら [Upload] をクリックします。
[Enter License Text] チェックボックス	このチェックボックスをオンにして、ライセンス テキストをコピーして貼り付けます。

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。

ライセンス監査の実行

ライセンス監査を実行する場合は、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。 ライセンスを更新するには、ライセンスの更新, （6 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 [ライセンス監査の実行] ダイアログボックスで、[送信] をクリックします。
監査が開始され、完了までには時間がかかる場合があります。
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。

システム情報の管理

[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。

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 [メール設定] 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（保存）] 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。

システム タスクの管理

システム タスクを管理する場合は、次の手順を実行します。

（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）ドロップダウン リストから [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。 • default-system-task-policy • local-run-policy
[時間] ドロップダウン リスト	ドロップダウンリストから時間単位の頻度を選択します。
[分] ドロップダウン リスト	ドロップダウンリストから頻度を指定する数字を選択します。 （注） このドロップダウン リストは、特定のシステム タスクに対してのみ表示されます。

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。

電子メール アラートの設定

重大な障害に対する電子メールアラートを設定するには、次の手順を実行します。 この設定により、対象となる受信者はすべてのサーバで記録された一連の障害をまとめて電子メールで受け取ります。

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。
ステップ 3 [Email Alert Rule Setting] 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
[Email Addresses] フィールド	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。
[Enable Alert] 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。

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。

ユーザ ロールの管理

ユーザ ロールの追加

デフォルトでは、オペレータ ロールおよび管理者ロールを Cisco IMC Supervisor で使用できます。新しいユーザ ロールを追加する場合は、次の手順を実行します。

手順

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

ステップ 2 [ユーザロール] 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の [User Role] ペインで、次の手順を実行します。

フィールド	説明
[ユーザロール] フィールド	ユーザ ロールの記述名。
[ロールタイプ] ドロップダウン リスト	リストから [Admin] または [End User] を選択します。
[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。

ユーザ ロールの編集

既存のユーザ ロールを編集するには、次の手順を実行します。

はじめる前に

既存のユーザ ロールが必要です。

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 [ユーザロール] タブをクリックします。

ステップ 3 ユーザ ロールのリストから、編集するユーザ ロールを選択します。

ステップ 4 [Edit] をクリックします。

（注） リストからユーザ ロールを選択するまでは、[Edit] ボタンは表示されません。

ステップ 5 [Next] をクリックします。

（注） [User Role]、[Role Type]、[Description] は編集できません。

ステップ 6 [Next] をクリックします。

ステップ 7 [Menu Settings] ペインで、要件に従って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またはオフにします。

ステップ 8 [Next] をクリックします。

ステップ 9 [User Permissions] ペインで、要件に応じて操作フィールドの横のチェックボックスをオンまたはオフにします。

ステップ 10 [Submit] をクリックします。

ステップ 11 確認ダイアログボックスで、[OK] をクリックします。

ユーザ ロールの複製

既存のユーザ ロールを複製するには、次の手順を実行します。

はじめる前に

既存のユーザ ロールが必要です。

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 [ユーザロール] タブをクリックします。

ステップ 3 ユーザ ロールのリストから、複製するユーザ ロールを選択します。

ステップ 4 [Clone] をクリックします。

（注） リストからユーザ ロールを選択するまでは、[Clone] ボタンは表示されません。

ステップ 5 [Clone User Role] ダイアログボックスの [User Role] ペインで、次の手順を実行します。

フィールド	説明
[ユーザロール] フィールド	ユーザ ロールの記述名。
[ロールタイプ] ドロップダウン リスト	リストから [Admin] または [End User] を選択します。
[Description] フィールド	（オプション）ユーザ ロールの説明。

ステップ 6 [Next] をクリックします。

ステップ 7 [Menu Settings] ペインで、要件に従って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またはオフにします。

ステップ 8 [Next] をクリックします。

ステップ 9 [User Permissions] ペインで、要件に応じて操作フィールドの横のチェックボックスをオンまたはオフにします。

ステップ 10 [Submit] をクリックします。

ステップ 11 確認ダイアログボックスで、[OK] をクリックします。

ユーザ ロールの削除

既存のユーザ ロールを削除するには、次の手順を実行します。

はじめる前に

既存のユーザ ロールが必要です。

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 [ユーザロール] タブをクリックします。
ステップ 3 ユーザ ロールのリストから、削除するユーザ ロールを選択します。
ステップ 4 [Delete] をクリックします。
（注） リストからユーザ ロールを選択するまでは、[Delete] ボタンは表示されません。
ステップ 5 [Delete User Role] ダイアログボックスで、[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。

ユーザの管理

ログイン ユーザの管理

ログイン ユーザの追加

新しいログイン ユーザを追加する場合は、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Administration] > [Users] を選択します。
ステップ 2 [ログインユーザ] 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	[Operator] または [System Admin] を選択します。
[ログイン名] 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。
[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。

フィールド	説明
[User Contact Email（ユーザの連絡先電子メール）] 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）ユーザの住所。

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。

ログイン ユーザの編集

ログイン ユーザを編集する場合は、次の手順を実行します。

はじめる前に

ログイン ユーザ グループは、[Login Users] 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、[Administration] > [Users] を選択します。

ステップ 2 [ログインユーザ] タブをクリックします。

ステップ 3 ログイン ユーザのリストから、編集するユーザを選択します。

ステップ 4 [Edit] をクリックします。

ステップ 5 [Edit User] 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
[User Contact Email（ユーザの連絡先電子メール）] 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。

フィールド	説明
[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）ユーザの住所。

（注） [User Role] および [Login Name] のユーザの詳細は編集できません。

ステップ 6 [Save（保存）] をクリックします。

ステップ 7 [OK] をクリックします。

ログイン ユーザの削除

ログイン ユーザを削除する場合は、次の手順を実行します。

はじめる前に

ログイン ユーザ グループは、[Login Users] 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、[Administration] > [Users] を選択します。

ステップ 2 [ログインユーザ] タブをクリックします。

ステップ 3 ログイン ユーザのリストから、削除するユーザを選択します。

ステップ 4 [Delete] をクリックします。

ステップ 5 [Delete User] ダイアログボックスで、[Delete] 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。

ユーザ パスワードの変更

ログイン ユーザのパスワードを変更する場合は、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Administration] > [Users] を選択します。
ステップ 2 [ログインユーザ] タブをクリックします。
ステップ 3 ユーザのリストから、パスワードを変更するユーザ ロールを選択します。
ステップ 4 [Change Password] をクリックします。
ステップ 5 [Change Password] 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
[New Password] フィールド	新しいパスワードを入力します。
[Confirm Password] フィールド	新しいパスワードを再度入力します。

ステップ 6 [Save（保存）] をクリックします。
ステップ 7 [OK] をクリックします。

ブランディング ページの管理

新しいログイン ブランディングの追加

新しいログイン ユーザを追加する場合は、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Administration] > [Users] を選択します。
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] ドロップダウン リスト	ドメインの記述名。

フィールド	説明
[Custom Domain Logo] チェックボックス	（オプション）ロゴを追加する場合は、このチェックボックスをオンにして、以下を実行します。 1 [Browse] をクリックします。 2 ロゴに移動してファイルを選択します。 3 [Open] 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 確認ダイアログボックスで、[OK] をクリックします。

ブランディング ページの編集

ブランディング ページのロゴを編集する場合は、次の手順を実行します。 ブランディング ページの名前は変更できません。

はじめる前に

ユーザ定義のブランディング ページがすでに作成されている必要があります。

手順

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

ステップ 2 [Login Page Branding] タブをクリックします。

ステップ 3 ブランディング ページのリストから、編集するページを選択します。

ステップ 4 [Edit] をクリックします。

（注） リストからページを選択するまでは、[Edit] ボタンは表示されません。

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

1 [Custom Domain Logo] チェックボックスをオンにします。
2 [Browse] をクリックします。
3 ロゴに移動してファイルを選択します。
4 [Open] 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。

ブランディング ページの複製

ブランディング ページを複製する場合は、次の手順を実行します。

はじめる前に

ユーザ定義のブランディング ページがすでに作成されている必要があります。

手順

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

ステップ 2 [Login Page Branding] タブをクリックします。

ステップ 3 ブランディング ページのリストから、複製するページを選択します。

ステップ 4 [Clone] をクリックします。

（注） リストからページを選択するまでは、[Clone] ボタンは表示されません。

ステップ 5 [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] ドロップダウン リスト	ドメインの記述名。
[Custom Domain Logo] チェックボックス	（オプション）ロゴを追加する場合は、このチェックボックスをオンにして、以下を実行します。 1 [Browse] をクリックします。 2 ロゴに移動してファイルを選択します。 3 [Open] 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。

認証設定の管理

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 バーで、[Administration] > [Users] を選択します。

ステップ 2 [Authentication Preferences] ドロップダウン リストから認証タイプを選択します。
次のオプションを使用できます。

- [Local Authentication]：この認証設定を使用すると、LDAP ユーザは、Cisco IMC Supervisor にログインできません。 ステップ ステップ 4 に進みます。
- [Local First, fallback to LDAP]：このオプションを選択した場合、LDAP 統合を設定する必要があります。 x を参照してください。 ステップ ステップ 4 に進みます。
- [LDAP First, fallback to local]：このオプションを選択した場合、LDAP 統合を設定する必要があります。 x を参照してください。 ステップ ステップ 4 に進みます。
- [Verisign Identity Protection]：このオプションを選択した場合は、ステップ ステップ 3 に進みます。

ステップ 3 [Verisign Identity Protection] を選択した場合は、次の手順を実行します。

1. VIP 証明書をアップロードするには、[参照] をクリックします。 証明書を見つけて選択し、[アップロード] をクリックします。
2. パスワードを入力します。

ステップ 4 [Save（保存）] をクリックします。

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 同期はシステム タスクとしても実行できます。 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。

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。

LDAP 統合の規則と制限事項

ユーザの同期規則

- 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 [ローカル] 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 [外部] 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。
- LDAP ディレクトリの同期後、LDAP 外部ユーザは完全なドメイン名と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。

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になります。

（注） LDAP同期プロセスの後には、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てください。

LDAP サーバのサマリー情報の表示

手順

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

ステップ 2 [LDAP統合] タブを選択します。

ステップ 3 表から LDAP アカウント名を選択します。

ステップ 4 [表示] をクリックします。
[View LDAP Account Information（LDAP アカウント情報の表示）] ダイアログボックスに、LDAP アカウントのサマリー情報が表示されます。

ステップ 5 [閉じる] をクリックします。

LDAP サーバの接続のテスト

手順

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

ステップ 2 [LDAP統合] 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 [テスト接続] をクリックします。

ステップ 5 [Test LDAP Connectivity（LDAP 接続のテスト）] ダイアログボックスで、[閉じる] をクリックします。

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
- 検索ベース DN の選択内容

手順

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

ステップ 2 [LDAP統合] タブをクリックして、LDAP アカウントを選択します。

ステップ 3 [変更] をクリックします。

ステップ 4 [LDAPサーバ設定の変更] ペインで、次のフィールドを編集します。

名前	説明
[SSLの有効化] 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。
[ポート] 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。

名前	説明
[ユーザ名] 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。 uid=users,ou=People,dc=ucsd,dc=com ここに指定する ou 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。
[パスワード] フィールド	ユーザのパスワード。

ステップ 5 [次へ] をクリックします。

ステップ 6 [LDAP検索ベース] ペインで、[選択] をクリックして LDAP 検索ベースのエントリを指定し、[選択] をクリックします。

ステップ 7 [送信] 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。

手順

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

ステップ 2 [LDAP統合] 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 [削除] 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 [削除] 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。 [更新] 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。

ユーザ パスワード ポリシーの管理

ユーザ パスワード ポリシーを変更する場合は、次の手順を実行します。

手順

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

ステップ 2 [Password Policy] タブをクリックします。

ステップ 3 [Minimum Password Length] では、ドロップダウン リストから値を選択します。

ステップ 4 [Maximum Password Length] では、ドロップダウン リストから値を選択します。

ステップ 5 [Minimum Character Classes] では、ドロップダウン リストから値を選択します。

ステップ 6 （任意） [Disallow Login in Password] チェックボックスをオンにすると、ユーザはログイン テキストをパスワードとして使用できなくなります。

ステップ 7 （任意） [Disallow Previouis Password] チェックボックスをオンにすると、ユーザはパスワードの変更時に同じパスワードを再使用できなくなります。

ステップ 8 （任意） [Disallow Password that match Regular Expression] では、ユーザにパスワードとして選択させない共通表現を入力します。 各表現の先頭に # を付けます。

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。

統合の管理

[CMDB Integration Setup] の設定

構成管理データベース（CMDB）は、システムの変更を追跡および管理するために使用されます。CMDB には通常、サービス リクエスト、グループなどのリソースに対する追加、削除、または変更のイベント タイプが表示されます。

CMDB 統合を設定するか、設定を変更する場合は、次の手順を実行します。

手順

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

ステップ 2 [CMDB統合設定] タブを選択し、次のフィールドに値を入力します。

フィールド	説明
[Export to FTP Server] チェックボックス	FTP サーバに変更記録をエクスポートするには、このチェックボックスをオンにします。
[Export Format] ドロップダウン リスト	リストから [CSV] または [XML] を選択します。
[FTP Server] フィールド	FTP サーバの IP アドレス。
[FTP Port] フィールド	（オプション）FTP サーバのポート番号。
[FTP User] フィールド	（オプション）FTP サーバのユーザ名。
[FTP Server] フィールド	FTP サーバのユーザ パスワード。
[FTP Export Frequency] ドロップダウン リスト	ドロップダウン リストから頻度を選択します。
[FTP File Name] フィールド	FTP サーバのユーザ パスワード。
[Test FTP] チェックボックス	FTP の設定をテストするには、このチェックボックスをオンにします。

ステップ 3 [Save（保存）] をクリックします。

監査ログの表示

Cisco IMC Supervisor は最大 10000 個の監査ログを保存できます。 ログの数が 10000 を超えると、24 時間ごとに実行される CMDB 10K Records Purge Task によって古いログが消去されます。

監査ログを表示する場合は、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] > [Integration] を選択します。

ステップ 2 [レコードの変更] タブを選択します。
次のレコードを使用できます。

フィールド	説明
ID	ログのシリアル番号。

フィールド	説明
Change Time	変更が行われたシステム時刻。
Change Type	変更のタイプ（ADD、MODIFY、または DELETE）
Resource Type	リソースのタイプ。
Change by User	ログイン ユーザ名。
Resource Name	リソースの IP アドレスまたは名前。
Description	ログの説明。
Additional Details	ログに関するその他の詳細。

（注） 1ページに表示するレコード数をカスタマイズできます。ページの右下隅にあるドロップダウン リストをクリックして、1ページに表示するレコード数をリストから選択します。

[User Interface Settings] の設定

Cisco IMC Supervisor のヘッダー タイトルおよび他のヘッダー オプションを更新するには、次の手順を使用します。

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。
[Product Name 2nd Line] フィールド	ヘッダーのサブタイトル。

フィールド	説明
[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。
管理者ポータル	
[Custom Link 1 Lable] 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。
[カスタムリンク1の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 Lable] 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。
[カスタムリンク2の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。
エンド ユーザ ポータル	
[Custom Link 1 Lable] 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。
[カスタムリンク1の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 Lable] 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。
[カスタムリンク2の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（保存）] 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。

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 *1*：基本情報および詳細情報

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。
	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 *2*：ログの表示

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 *3*：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 *4*：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	1 [Debug Logging] を選択して [Start Debug Logging] をクリックします。 2 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。

第 6 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，75 ページ
- その他の手順，76 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	Cisco IMC Supervisor の起動，（5 ページ）
ライセンスの更新方法	ライセンスの更新，（6 ページ）
Cisco IMC Supervisor にログイン ユーザを追加する方法	ログイン ユーザの追加，（58 ページ）
ラック グループの追加方法	ラック グループの追加，（6 ページ）
ラック アカウントの作成方法	ラック アカウントの追加，（7 ページ）

その他の手順

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す。

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（保存）] 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（保存）] 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 ステップ 3 とステップ ステップ 4 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。