



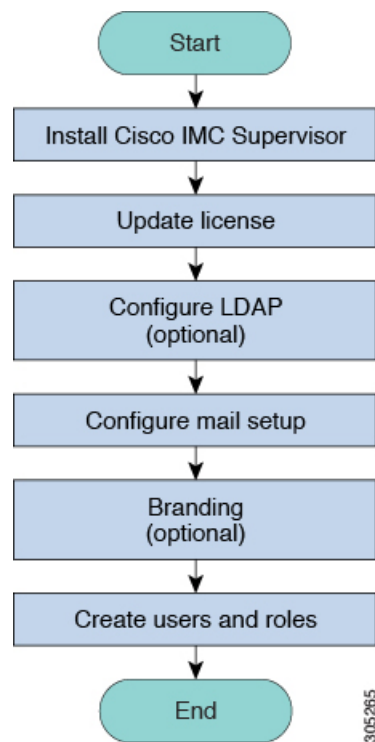
はじめに

この章は次のトピックで構成されています。

- [概要](#) (1 ページ)
- [起動 Cisco IMC Supervisor](#) (2 ページ)
- [ライセンス タスク](#) (3 ページ)
- [ユーザ アクセス プロファイルの管理](#) (6 ページ)
- [認証および LDAP 統合](#) (9 ページ)
- [LDAP の設定](#) (10 ページ)
- [SCP ユーザの設定](#) (24 ページ)
- [電子メール設定の設定](#) (24 ページ)
- [Cisco.com ユーザ資格情報とプロキシ設定](#) (25 ページ)
- [CMDB 統合の設定](#) (27 ページ)
- [ブランディング](#) (28 ページ)
- [ユーザ インターフェイス設定の設定](#) (29 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。



起動 Cisco IMC Supervisor

Cisco IMC Supervisor が、正しく設定された IP アドレスを使用してインストールされている必要があります。

始める前に

- 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 のインストール時に IP アドレスが設定されていることを確認します。

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。

- [ユーザ名 (User Name)] : **admin**
 - [パスワード (Password)] : **admin**
-

ログインすると 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が表示されます。

ライセンス タスク

[ライセンス (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状況を表示できます。次のライセンス手順は、[管理 (Administration)]>[ライセンス (License)]メニューから実行できます。

タブ	説明
[ライセンス キー (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。このタブでは、ライセンスを更新、交換、移行することもできます。Cisco IMC Supervisor の新しいバージョンが利用可能になったら、ライセンスを更新できます。
[ライセンス使用率 (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。 (注) Cisco IMC Supervisor のライセンスはサーバの数に基づきます。Cisco UCS S3260 シャーシは2サーバノードです。このため Cisco IMC Supervisor では、このシャーシのライセンス使用数が2サーバとして見なされます。
[リソース使用率のデータ (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せん。
非アクティブ化されたライセンス	このタブには、非アクティブにされたライセンスのリストが表示されます。

ライセンスの更新

Cisco IMC Supervisor の使用を開始する前に、次の手順を実行してライセンスを更新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](#)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 キーを請求及び登録します。Cisco IMC Supervisor のインストールが完了すると、ライセンスが検証されているため、Cisco IMC Supervisor を使用できます。

始める前に

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 [管理 (Administration)] > [ライセンス (License)] の順に選択します。

ステップ 2 [ライセンス (License)] ページで [ライセンス キー (License Keys)] を選択します。

ステップ 3 [ライセンス キー (License Keys)] ページで [ライセンスの更新 (Update License)] をクリックします。

ステップ 4 [ライセンスの更新 (Update License)] 画面で次のいずれかの操作を行います。

- **.lic** ファイルをアップロードするには、[参照 (Browse)] をクリックして **.lic** ファイルを探して選択してから、[アップロード (Upload)] をクリックします。
- ライセンスキーの場合は、[ライセンステキストの入力] 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 [ライセンステキスト] 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 [ライセンステキスト (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 [送信 (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。

ライセンスの置換

システムでライセンスを置換するには、この手順を使用します。この操作を行うと、システムのその他の既存のライセンスが非アクティブになります。

手順

ステップ 1 [管理 (Administration)] > [ライセンス (License)] の順に選択します。

ステップ 2 [ライセンス (License)] ページで [ライセンス キー (License Keys)] を選択します。

ステップ 3 [ライセンスの交換 (Replace License)] を選択します。

ステップ 4 [ライセンスのアップロード (Upload License)] フィールドで、PAK ファイルをドラッグアンドドロップするか、または [ファイルを選択 (Select a File)] をクリックしてファイルを参照して選択します。

ステップ 5 (任意) [ライセンステキストの入力 (Enter License Text)] をオンにし、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 6 [送信 (Submit)] をクリックします。

既存のライセンスはすべて新しいライセンスに置き換えられます。

非アクティブ化されたライセンスの表示

非アクティブライセンスのリストはユーザ インターフェイスから表示できます。非アクティブライセンスに関する次の情報を表示できます。

- PAK ファイル名
- ファイル ID
- ライセンス エントリ
- ライセンス値
- 有効期限日
- 非アクティブ化された時刻
- ライセンスを非アクティブ化したユーザの名前

手順

ステップ 1 [管理 (Administration)] > [ライセンス (License)] の順に選択します。

ステップ 2 [ライセンス (License)] ページで [非アクティブ化されたライセンス (Deactivated Licenses)] を選択します。

ステップ 3 すべての非アクティブライセンスに関して表示された情報を確認します。

ライセンスの移行

Cisco IMC Supervisor では、グラフィカル ユーザ インターフェイスを使用してライセンスを移行できます。たとえば、永久ライセンスからサブスクリプションライセンスに移行できます。

手順

ステップ 1 [管理 (Administration)] > [ライセンス (License)] の順に選択します。

ステップ 2 [ライセンス (License)] ページで [ライセンス キー (License Keys)] を選択します。

ステップ 3 [ライセンス キー (License Keys)] ページで [ライセンスの移行 (Migrate License)] をクリックします。

- ステップ 4** [ライセンスのアップロード (Upload License)] フィールドで、PAK ファイルをドラッグアンドドロップするか、または [ファイルを選択 (Select a File)] をクリックしてファイルを参照して選択します。
- ステップ 5** (任意) [ライセンス テキストの入力 (Enter License Text)] をオンにし、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 6** [送信 (Submit)] をクリックします。
-

ライセンス監査の実行

ライセンスの監査を実行するには、この手順を実行します。

始める前に

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 \(3 ページ\)](#) を参照してください。

手順

- ステップ 1** [管理 (Administration)] > [ライセンス (License)] の順に選択します。
- ステップ 2** [ライセンス (License)] ページで [ライセンス使用率 (License Utilization)] をクリックします。
- ステップ 3** [その他の操作 (More Actions)] ドロップダウンリストから [ライセンス監査の実行 (Run License Audit)] を選択します。
- ステップ 4** [ライセンス監査の実行 (Run License Audit)] 画面で、[送信 (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。
-

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 IMC Supervisor 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。

LDAP ユーザを Cisco IMC Supervisor 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) [プロファイルの管理 (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** [管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択します。
- ステップ 2** [ユーザとグループ (Users and Groups)] ページで [ユーザ (User)] をクリックします。
- ステップ 3** リストからユーザを選択します。
- ステップ 4** [その他の操作 (More Actions)] ドロップダウンリストから [プロファイルの管理 (Manage Profiles)] を選択します。
- ステップ 5** [プロファイルの管理 (Manage Profile)] ページで、[追加+ (Add +)] をクリックします。
- ステップ 6** [アクセス プロファイルへのエントリの追加 (Add Entry to Access Profiles)] ページで、次のフィールドに入力します。

フィールド名	説明
[名前 (Name)] フィールド	プロファイル名。
[説明 (Description)] フィールド	プロファイルの説明です。
[タイプ (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。
[顧客組織 (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。
[ユーザがアクセスできる他のすべてのグループからのリソースを表示 (Show Resources From All Other Groups the User Has Access)] チェックボックス	ユーザがアクセス可能なまたはユーザが属している他のすべてのグループからのリソースを表示できるように指定する場合に、このチェックボックスをオンにします。
[共有グループ (Shared Groups)] フィールド	[選択 (Select)] をクリックして、ユーザ プロファイ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。
[デフォルトプロファイル (Default Profile)] チェックボックス	デフォルトのユーザアクセス プロファイルである場合は、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 [送信 (Submit)]をクリックします。

次のタスク

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

システムのユーザは、自分のアカウントに複数のプロフィールが存在する場合は、特定のプロフィールを使ってシステムにログインできます。

手順

ステップ1 [Cisco IMC Supervisor ログイン (Cisco IMC Supervisor login)]ページの[ユーザ名 (Username)]フィールドに、ユーザ名を「ユーザ名: アクセス プロファイル名」の形式で入力します。

例 : Alex: GrpAdmin

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

ステップ3 [ログイン (Login)]をクリックします。

デフォルト プロファイル

デフォルト プロファイルは、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 プロファイ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、右上隅に表示されたユーザ名をクリックします。

ユーザ名は [ログアウト (logout)]オプションの左側に表示されます。

ステップ2 [ユーザ情報 (User Information)]ページの [アクセス プロファイル (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、[デフォルトプロフィールとして設定 (Set as Default Profile)]をクリックします。

(注) プロファイルは、追加時または編集時にデフォルトとして設定することもできます。

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 (VIP) 認証を設定できます。

名前	説明
ローカルが最初、LDAP にフォールバック (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 ID 保護 (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 [管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択します。

ステップ 2 [認証の環境設定 (Authentication Preferences)] を選択します。

ステップ 3 [認証の環境設定 (Authentication Preferences)] ドロップダウンリストから、次のいずれかのオプションを選択します。

- ローカルが最初、LDAP にフォールバック (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 \(15 ページ\)](#) を参照してください。

- [VeriSign ID 保護 (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 ID 保護 (Verisign Identity Protection)] を選択した場合は、次の手順を実行します。

- VIP 証明書をアップロードするには、[参照 (Browse)] 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 (Upload)] をクリックします。
- [パスワード (Password)] を入力します。

ステップ 5 [保存 (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。以降のセクションでは、これらの手順の実行方法について説明します。

LDAP の統合

LDAP 統合を使用して、LDAP サーバのユーザを Cisco IMC Supervisor と同期することができます。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 IMC Supervisor 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。

LDAP ディレクトリに新しい組織単位 (OU) を追加し、手動または自動で同期プロセスを実行している場合は、最近追加された 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。

[LDAP ユーザのクリーンアップ (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、[グループに属していないユーザ (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@vxedomain.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 [ローカル (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 [外部 (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。
- ユーザは複数の設定グループに属することができます。ただし、ユーザが属するグループのリストで最初に表示されているグループが、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 [ドメインユーザ (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、システムの指定された LDAP グループ、およびネストされたグループがあればそれも併せて取得されます。
- 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、[プロファイルの管理 (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、指定したフィルタと一致するすべてのユーザと、それらのユーザが属しているグループがシステムに取得されます。
- 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。ユーザプリンシパル名とプロファイル名の両方を使用した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 [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 ディレクトリで作成されている場合は、最初に同期された LDAP ディレクトリのユーザ詳細が表示されます。他の LDAP ディレクトリのユーザ詳細は表示されません。
- 複数の LDAP ディレクトリが同期された後、LDAP 外部ユーザは、完全なドメイン名をユーザ名と共に指定して Cisco IMC Supervisor にログインする必要があります。たとえば `vxdomain.cisco.com\username` のように指定します。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 と同期すると、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 と同期します。

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 [管理 (Administration)] > [LDAP 統合 (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 [LDAP 設定の追加 (Add LDAP Configurations)] ページで、次のフィールドに入力します。

フィールド	説明
[アカウント名 (Account Name)] フィールド	LDAP アカウント名。
[サーバタイプ (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。
[サーバ (Server)] フィールド	サーバのホスト名または IP アドレス。
[SSL の有効化 (Enable SSL)] チェックボックス	LDAP サーバに対するセキュアな接続を有効にします。

フィールド	説明
[ポート (Port)] フィールド	ポート番号 SSL では 636 に、非セキュア モードでは 389 に自動的に設定されます。
[ドメイン名 (Domain Name)] フィールド	LDAP ユーザのドメイン名。
[ユーザ名 (Username)] フィールド	LDAP ユーザの名前を入力します。
[パスワード (Password)] フィールド	ユーザ名に関連付けられるパスワードを入力します。
[同期頻度 (Synchronization Frequency)] ドロップダウンリスト	LDAPサーバを同期する頻度 (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"> • 1 • 4 • 12 • 24

ステップ 4 [次へ (Next)] をクリックします。

ステップ 5 [LDAP 検索ベース (LDAP Search Base)] ページで [選択 (Select)] をクリックし、表示されているテーブルから OU に基づいてユーザを取得するための検索条件を選択します。

(注) Cisco IMC Supervisor ではユーザはサポートされていますが、グループはサポートされていません。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)。システム同期タスクが 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 \(20 ページ\)](#) を参照してください。

ステップ 6 [選択 (Select)] ダイアログボックスで [選択 (Select)] をクリックします。

選択した検索条件が、[検索ベース (Search Base)] フィールドの横に表示されます。

ステップ 7 [LDAP 検索ベース (LDAP Search Base)] ダイアログボックスの [次へ (Next)] をクリックします。

ステップ 8 [+] をクリックし、[LDAP ユーザ ロール フィルタ (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します。

ステップ 9 [ユーザ ロール フィルタへのエントリの追加 (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 [送信 (Submit)] をクリックします。

これらのフィルタは編集または削除できます。また、上矢印と下矢印を使ってフィルタを移動して、フィルタの優先順位を設定できます。

- ステップ 11** [LDAP ユーザ ロール フィルタ (LDAP User Role Filter)] ダイアログボックスで、[送信 (Submit)] 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) に含まれている組織単位 (OU)。
- LDAP アカウントがシステムと自動的に同期される頻度。
- 結果を絞り込み、グループおよびユーザに 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。

始める前に

認証設定を [ローカルが最初、LDAP にフォールバック (Local First, fallback to LDAP)] に設定している必要があります。

手順

- ステップ 1** [管理 (Administration)] > [LDAP 統合 (LDAP Integration)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [LDAP サーバの設定 (LDAP Server Configuration)] ページで、次のフィールドに入力します。

名前	説明
[アカウント名 (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。
[サーバタイプ (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"> • OpenLDAP • MSAD - Microsoft Active Directory
[サーバ (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
[SSLの有効化 (Enable SSL)] チェックボックス	LDAP サーバに対するセキュアな接続を有効にします。
[ポート (Port)] フィールド	ポート番号 SSL では 636 に、非セキュア モードでは 389 に自動的に設定されます。
[ドメイン名 (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。 重要 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。
[ユーザ名 (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ます。 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 (Password)] フィールド	ユーザのパスワード。
[同期頻度 (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"> • 1 • 4 • 12 • 24

ステップ 4 [次へ (Next)] をクリックします。

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

このリストには、Cisco IMC Supervisor で利用できるすべての組織単位 (OU) が表示されます。

ステップ 6 [次へ (Next)] をクリックします。

ステップ7 [ユーザとグループのフィルタの設定 (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
ユーザフィルタ (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。
グループフィルタ (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、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。
[ユーザフィルタへのエントリの追加 (Add Entry to User Filters)] または [グループフィルタへのエントリの追加 (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)	
[属性名 (Attribute Name)] ドロップダウンリスト	[グループ名 (Group Name)] または [ユーザ名 (User Name)] を選択します。
[オペレータ (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"> • 等しい (Equals to) • 開始 (Starts with)
[属性値 (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 [次へ (Next)] をクリックします。

ステップ9 [LDAP ユーザロールフィルタ (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 [ユーザロールフィルタへのエントリの追加 (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
[属性名 (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。
[オペレータ (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"> • 次の値と等しい (Equal to) • 開始 (Starts with)
[属性値 (Attribute Value)] フィールド	このフィールドで値を指定します [オペレータ (Operator)] フィールドと [属性値 (Attribute Value)] フィールドの値に一致するすべてのユーザが、[ユーザロールのマッピング (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。
[ユーザロールのマッピング (Map User Role)] ドロップダウンリスト	ユーザのマッピング先とするユーザ ロールを選択します。デフォルトのロールまたはユーザ定義のロールを選択できます。 Cisco IMC Supervisor に用意されているデフォルトのロールは以下のとおりです。 <ul style="list-style-type: none"> • グループ管理者 • 演算子 • システム管理者 (System Admin)

ステップ 11 [送信 (Submit)] をクリックします。

ユーザ ロール フィルタが [ユーザ ロール フィルタ (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、最初の行のフィルタが適用されます。

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

次のタスク

LDAP に認証の環境設定を設定していない場合は、認証の環境設定を変更するように指示されます。 [認証の環境設定 \(9 ページ\)](#) を参照してください。

LDAP サーバのサマリー情報の表示

LDAP サーバのサマリー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 [管理 (Administration)] > [LDAP 統合 (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 [表示 (View)] をクリックします。

[LDAP アカウント情報の表示 (View LDAP Account Information)] 画面に、LDAP アカウントのサマリー情報が表示されます。

ステップ 4 [閉じる (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 [管理 (Administration)] > [LDAP 統合 (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 [テスト接続 (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 [LDAP 接続のテスト (Test LDAP Connectivity)] ダイアログボックスで、[閉じる (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 [管理 (Administration)] > [LDAP 統合 (LDAP Integration)] を選択します。

ステップ 2 [ベースDNの検索 (Search BaseDN)] をクリックします。

(注) Cisco IMC Supervisor ではユーザはサポートされていますが、グループはサポートされていません。**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)。

- ステップ 3** [LDAP 検索ベース (LDAP Search Base)] ダイアログボックスで [選択 (Select)] をクリックします。
- ステップ 4** [選択 (Select)] ダイアログボックスで、1 つ以上のユーザを選択して [選択 (Select)] をクリックします。
- ステップ 5** [LDAP 検索ベース (LDAP Search Base)] ダイアログボックスで [送信 (Submit)] 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** [管理 (Administration)] > [LDAP 統合 (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** [LDAP の手動同期のリクエスト (Request Manual LDAP Sync)] ページで、次のフィールドに情報を入力します。

名前	説明
[基本検索 (Basic Search)] チェックボックス	組織単位ごとの基本検索を可能にします。
[詳細検索 (Advanced Search)] チェックボックス	詳細検索を可能にします。

(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 に存在する場合、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、[選択 (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、[選択 (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、[詳細なフィルタオプション (Advanced Filtering Options)] ペインで、[ユーザフィルタ (User Filters)] と [グループフィルタ (Group Filters)] の属性名を追加または編集します。
- ステップ 7** [次へ (Next)] をクリックします。

ステップ 8 [ユーザとグループの選択 (Select Users and Groups)] ページで、次のフィールドに入力します。

名前	説明
[LDAP グループ (LDAP Groups)] フィールド	ユーザを同期する必要がある LDAP グループ。
[LDAP ユーザ (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 [送信 (Submit)] をクリックします。

[管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択し、[ユーザ (Users)] をクリックして同期されたユーザを確認します。

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 [管理 (Administration)] > [システム (System)] を選択します。

ステップ 2 [システム (System)] ページで [システムのタスク (System Tasks)] をクリックします。

ステップ 3 [ユーザとグループのタスク (User and Group Tasks)] を展開し、[LDAPSycTask] を選択します。

ステップ 4 [今すぐ実行 (Run Now)] をクリックします。

ステップ 5 [送信 (Submit)] をクリックします。

ステップ 6 (オプション) [タスクの管理 (Manage Task)] をクリックして、同期処理を有効または無効にします。

次のタスク

同期プロセスの結果が Cisco IMC Supervisor に表示されます。[LDAP 統合 (LDAP Integration)] ページで LDAP アカウントを選択し、[結果 (Results)] をクリックすると、同期プロセスの概要が表示されます。

LDAP サーバの詳細の変更

構成済み LDAP サーバで変更できる詳細は以下のみです。

- ポート番号および SSL 設定
- ユーザ名およびパスワード

- 同期頻度
- 検索ベース DN の選択
- 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** [管理 (Administration)] > [LDAP 統合 (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** [変更 (Modify)] をクリックします。
- ステップ 4** [LDAP サーバの設定 (LDAP Server Configuration)] ページで、次のフィールドを編集します。

名前	説明
[SSLの有効化 (Enable SSL)] チェックボックス	LDAP サーバに対するセキュアな接続を有効にします。
[ポート (Port)] フィールド	ポート番号 SSL では 636 に、非セキュア モードでは 389 に自動的に設定されます。
[ユーザ名 (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ます。 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 (Password)] フィールド	ユーザのパスワード。
[同期頻度 (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"> • 1 • 4 • 12 • 24

- ステップ 5** [次へ (Next)] をクリックします。

- ステップ6 [LDAP 検索ベース (LDAP Search Base)] エントリを編集し、[次へ (Next)] をクリックします。
- ステップ7 [ユーザフィルタ (User Filters)] および [グループフィルタ (Group Filters)] テーブルで必要な属性を選択して編集し、[次へ (Next)] をクリックします。
- ステップ8 [LDAP ユーザ ロール フィルタ (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 [送信 (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、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 [ドメインユーザ (Domain Users)] として設定されます。[プロファイルの管理 (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 IMC Supervisor 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 [管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択します。
- 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 [グループメンバーシップ (Group Membership)] をクリックします。
[以下のメンバー (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 [閉じる (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 サーバの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 [管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択します。
- ステップ2 [LDAP 統合 (LDAP Integration)] 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 (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 [削除] をクリックします。

それにより、Cisco IMC Supervisor 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の数によっては、この削除プロセスは完了するまで数分かかる場合があります。その間、LDAP アカウントは Cisco IMC Supervisor で表示されたままになります。[更新 (Refresh)] をクリックして、アカウントの削除を確定します。

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 SupervisorUI または shelladmin へのログインには使用できません。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 [管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択します。
 - ステップ2 [SCP ユーザ設定 (SCP User Configuration)] をクリックします。
 - ステップ3 [パスワード (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 [送信 (Submit)] をクリックします。
-

電子メール設定の設定

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](#)を参照してください。

手順

- ステップ 1 [管理 (Administration)] > [システム (System)] を選択します。
- ステップ 2 [電子メール設定 (Mail Setup)] をクリックします。
- ステップ 3 [電子メール設定 (Mail Setup)] ページで、次のフィールドに入力します。

フィールド	説明
送信電子メール サーバ (SMTP) (Outgoing Email Server (SMTP))	サーバの IP アドレスまたはドメイン名。
送信 SMTP ポート (Outgoing SMTP Port)	SMTP サーバのポート番号。
送信 SMTP ユーザ (Outgoing SMTP User)	(オプション) SMTP 認証で使用する送信 SMTP ユーザ ID。
送信 SMTP パスワード (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。
送信者の電子メールアドレス (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。
サーバIPアドレス	Cisco IMC Supervisor を実行しているサーバの IP アドレス。
[テストメールの送信 (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 [保存 (Save)] をクリックします。

Cisco.com ユーザ資格情報とプロキシ設定

[管理 (Administration)] > [システム (System)] から、Cisco ユーザ資格情報とプロキシの詳細を設定することができます。Cisco.com ユーザとプロキシの資格情報は、アプリケーション全体の設定です。これらの資格情報は、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 ユーザの名前と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 [管理 (Administration)] > [システム (System)] を選択します。

ステップ 2 [システム (System)] ページで、[Cisco.com ユーザ設定 (Cisco.com User Configuration)] をクリックします。

ステップ 3 Cisco.com ユーザを設定するため、次のフィールドに情報を入力します。

フィールド	説明
[ユーザ名 (cisco.com) (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。
[パスワード (cisco.com) (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 [保存 (Save)] をクリックします。

プロキシ設定

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 [管理 (Administration)] > [システム (System)] を選択します。

ステップ 2 [システム (System)] ページで、[プロキシ設定 (Proxy Configuration)] をクリックします。

ステップ 3 プロキシ設定の次のフィールドに入力します。

フィールド	説明
[プロキシ設定の有効化 (Enable Proxy Configuration)] チェックボックス	<p>(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を有効化し、次の情報を入力します。</p> <ul style="list-style-type: none"> • [ホスト名 (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。 • [ポート (Port)] フィールド: プロキシ設定用のポートを入力します。

フィールド	説明
[プロキシ認証の有効化 (Enable Proxy Authentication)] チェックボックス	<p>(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、次の情報を入力します。</p> <ul style="list-style-type: none"> • [プロキシユーザ名 (Proxy UserName)] 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。 • [プロキシパスワード (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。

ステップ4 [保存 (Save)] をクリックします。

CMDB 統合の設定

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。

手順

ステップ1 [管理 (Administration)] > [統合 (Integration)] を選択します。

ステップ2 [統合 (Integration)] ページで [CMDB 統合の設定 (CMDB Integration Setup)] をクリックします。

ステップ3 [CMDB 統合の設定 (CMDB Integration Setup)] 画面で、次を含む必須フィールドに入力します。

名前	説明
[FTP サーバにエクスポート] 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。
[エクスポート形式 (Export Format)] ドロップダウンリスト	エクスポート形式の種類 (CSV または XML) を選択します。
[FTP Server] フィールド	FTP サーバのアドレス。
[FTP Port] フィールド	FTP サーバ ポート番号。
[FTP User] フィールド	FTP ユーザ ID。
[FTP パスワード] フィールド	FTP ユーザ パスワード。

名前	説明
[FTP Export Frequency] ドロップダウンリスト	変更記録を FTP サーバにエクスポートする頻度を選択します。
[FTP File Name] フィールド	エクスポートされる変更記録のファイル名。 ファイルがターゲットFTPサーバにエクスポートされるたびに、次の変数を使用して新しいファイル名を作成できます。 MONTH、WEEK、DAY、YEAR、HOUR、MIN、SEC、MLLIS 例：XYZ-\$DAY-\$HOUR-\$MIN-\$SEC
[FTP のテスト] 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4 [保存 (Save)] をクリックします。

ブランディング

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 [管理 (Administration)] > [ユーザとグループ (Users and Groups)] を選択します。

ステップ2 [ログイン ページのブランディング (Login Page Branding)] をクリックします。

ステップ3 [追加 (Add)] をクリックします。

ステップ4 [ドメインブランディング (Domain Branding)] ページで、次のフィールドに入力します。

フィールド	説明
[ドメイン名 (Domain Name)] フィールド	ブランディング用ドメイン名。たとえば、imcs.xxxx.com です。 (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、10.10.10.10 imcs.xxxx.com です。
[カスタム ドメイン ロゴ (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. [参照 (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. [開く (Open)] をクリックします。

ステップ 5 [送信 (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、複製できます。

ユーザ インターフェイス設定の設定

Cisco IMC Supervisor アプリケーションをカスタマイズするには、次の手順を使用します。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 [管理 (Administration)] > [ユーザ インターフェイス設定 (Interface Settings)] を選択します。

ステップ 2 [ユーザ インターフェイス設定 (User Interface Settings)] ページで、次を実行します。

フィールド	説明
[ヘッダー全体の非表示] チェックボックス	ヘッダーを有効または無効にするには、このチェックボックスを使用します。
[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。
[バージョン情報ダイアログの有効化 (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 [バージョン情報 (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	
[カスタムリンク 1 のラベル (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。
[カスタムリンク1のURL (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。
[カスタムリンク 2 のラベル (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。
[カスタムリンク2のURL (Custom Link 1 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	
[カスタムリンク 1 のラベル (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。
[カスタムリンク1のURL (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。
[カスタムリンク 2 のラベル (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。
[カスタムリンク2のURL (Custom Link 1 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 [保存 (Save)] をクリックします。