管理

この章は、次の項で構成されています。

管理について

Cisco Business ダッシュボード の [Administration] オプションを使用すると、組織レベルでアプリケーションの動作を制御できます。このオプションは、次のページに分かれています。

- [Administration]：Cisco Business ダッシュボード に組織を作成し、管理します。
- [Device Groups]：ネットワークデバイスをグループに割り当てて、容易に管理できるようにします。
- [Device Credentials]：ネットワークデバイスにアクセスするときに使用するログイン情報を入力します。
- [Users]：Cisco Business ダッシュボード へのユーザアクセスを定義します。
- [Notification Defaults]：Cisco Business ダッシュボード のデフォルトの通知動作を変更します。
- [Notification Defaults]：Cisco Business ダッシュボード へのすべてのユーザアクセスのログを提供します。
- [Report Settings]：レポートの生成方法を制御する設定を変更します。

すべてのロールにすべてのページが表示されるわけではありません。オペレータはユーザ設定を管理できません。[Notification Defaults] と [Report Settings] は、管理者にのみ表示されます。

組織

組織は、ネットワーク、ユーザー、およびデバイスを、通常は個別に管理するグループに分割するために Cisco Business ダッシュボード で使用されます。各ネットワークまたはデバイスは 1 つの組織に属し、各ユーザーは 1 つ以上の組織を管理できます。組織は、顧客、部門または地域（会社にとって最も適切なもの）を表すことがありますが、どのような場合も、複数の組織を使用して、ネットワークのさまざまな部分を誰が表示し、管理できるかをより細かく制御できます。Cisco Business ダッシュボード のインストール時に、デフォルトと呼ばれる組織が 1 つ作成されます。

新しい組織を作成

1. **[Administration]** > **[Organizations]** に移動します。
2. テーブルの上部にある [+]（プラス）アイコンをクリックします。
3. 組織の名前を指定し、必要な詳細情報を入力します。
4. 新たに検出されたデバイスのデフォルトグループとして使用する必要がある新しいデバイスグループの名前を入力します。新しいデバイスグループが組織とともに作成されます。
5. 組織の変更期間の開始時刻と期間を指定します。
6. [Save] をクリックします。
7. 作成する組織ごとに上記の手順を繰り返します。

既存の組織を変更

1. [Administration] > [Organizations] に移動します。
2. 変更する組織のオプションボタンを選択し、[Edit] アイコンをクリックします。
3. 必要に応じて変更を加え、[Save] をクリックします。

組織の削除

1. [Administration] > [Organizations] に移動します。
2. 変更する組織のオプションボタンを選択し、[Deletion] アイコンをクリックします。

組織のモニタリングプロファイルを管理

モニタリングプロファイルを使用して、組織全体でのネットワーク デバイス モニタリングの実行方法を制御できます。組織レベルで選択されるプロファイルは、組織内のすべてのネットワークに適用されます。

組織のモニタリングプロファイルを変更するには、次の手順を実行します。

1. [Administration] > [Organizations] に移動します。
2. 変更する組織の名前をクリックし、[Monitoring Profiles] タブを選択します。
3. ドロップダウンを使用して、対応するタイプのデバイスに適用する適切なモニタリングプロファイルを選択します。モニタリングプロファイルの作成の詳細については、モニタリングプロファイル （11 ページ） を参照してください。

   また、個別のデバイスタイプまたは組織全体の [Inherit from Monitoring Defaults] チェックボックスをオンにして、システムレベルで定義されている動作に従うよう選択することもできます。
4. [Save] をクリックします。

（注） 実行可能なモニタリングのタイプとその管理方法の詳細については、「モニタリングプロファイル」を参照してください。システムレベルでのモニタリングプロファイルの変更に関する詳細については、モニタリングのデフォルト値 （11 ページ） を参照してください。

組織に関連付けられているユーザーを管理

組織管理者またはその下位のロールを持つユーザは、組織内のデバイスを表示または管理できるように、その組織に明示的に関連付ける必要があります。

ユーザーを組織に関連付けるには、以下の手順に従います。

1. [Administration] > [Organizations] に移動します。
2. 変更する組織の名前をクリックし、[Users] タブを選択します。
3. ✚（プラス）アイコンをクリックします。ドロップダウンリストからユーザーを選択します。

（注） [Administrator] レベルのユーザーは、すべての組織に暗黙的に関連付けられていて、ドロップダウンリストには表示されません。

組織からユーザーを削除するには、次の手順に従います。

1. [Administration] > [Organizations] に移動します。
2. 変更する組織の名前をクリックし、[Users] タブを選択します。
3. テーブル内のユーザの横にある [Delete] アイコンをクリックします。

組織に関連付けられているネットワークを管理

Cisco Business ダッシュボード 内のすべてのネットワークが単一の組織に属しています。[Organization Detail] ページの [Networks] タブを選択すると、組織に関連付けられているネットワークのリストを表示できます。

ネットワークと組織の関連付けは、ネットワークが最初に作成されたときに行われます。ネットワークが関連付けられている組織を変更するには、次の手順に従います。

1. [Network] に移動し、変更するネットワークを選択します。[More] をクリックして [Network Detail] パネルを表示します。
2. ネットワーク名の横にある [Edit] アイコンをクリックします。
3. ドロップダウンリストから新しい組織を選択します。
4. [OK] をクリックします。

このビューから、組織の新しいネットワークを作成できます。[+]（プラス）アイコンをクリックして新しいネットワークを作成し、表示されるフォームに適切な値を入力します。

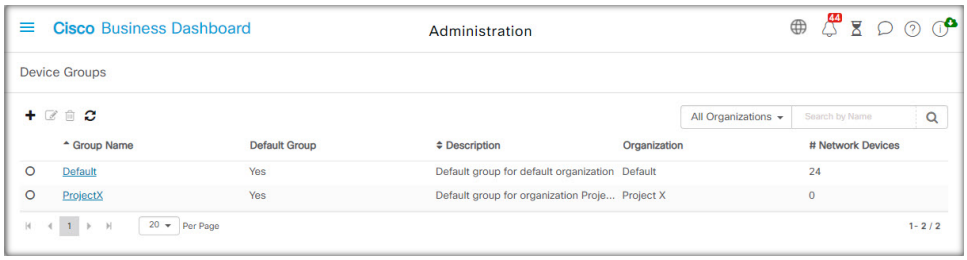
デバイスグループ

Cisco Business ダッシュボード は、ほとんどの設定タスクの実行にデバイスグループを使用します。複数のネットワークデバイスがグループ化されているため、デバイスのサブセットに対してのみ VLAN または WLAN を作成するなどの単一のアクションで構成できます。

各デバイス グループは複数の種類のデバイスを含むことができ、デバイス グループに設定が適用されると、その設定はグループ内のその機能をサポートするデバイスのみに適用されます。たとえば、デバイスグループにワイヤレスアクセスポイント、スイッチ、ルータが含まれている場合、新しいワイヤレス SSID の設定はワイヤレスアクセスポイントのみに適用され、ルータにはそれがワイヤレスルータである場合のみ適用されます。

デバイスグループには、複数のネットワークのデバイスが含まれている場合がありますが、すべてのデバイスが 1 つの組織に属している必要があります。デバイスグループは、組織またはネットワークのデフォルトのグループとして指定され、そのネットワークまたは組織で新たに検出されたデバイスがデフォルトのデバイスグループに配置されます。

デバイスグループの作成



1. [Administration] > [Device Groups] に移動します。

2. ✚（プラス）記号をクリックして新しいグループを作成します。
3. グループの組織、名前、および説明を入力します。[Save] をクリックします。
4. 必要に応じて、[+]（プラス）アイコンをクリックし、グループに追加するデバイスを検索ボックスを使用して選択し、デバイスをデバイス グループに追加します。デバイスは、個別に追加することも、ネットワーク別に追加することもできます。選択したデバイスがすでに別のグループのメンバーになっている場合は、そのグループから削除されます。各デバイスは、1 つのグループのみのメンバーになることができます。

デバイスグループの変更

1. [Administration] > [Device Groups] に移動します。
2. 変更するグループの横にあるオプション ボタンを選択し、[Edit] アイコンをクリックします。
3. 必要に応じて、名前と説明を変更します。[Save] をクリックします。
4. 必要に応じてデバイスをグループに追加または削除します。以前グループに追加したデバイスを削除するには、デバイスの横の**ゴミ箱**アイコンをクリックします。デバイスがネットワークまたは組織の [Default] グループに移動されます。

（注） [Default] グループからデバイスを削除することはできません。[Default] グループからデバイスを削除するには、デバイスを新しいグループに追加する必要があります。

デバイスグループの削除

1. [Administration] > [Device Groups] に移動します。
2. 削除するデバイスグループのオプションボタンをクリックし、[Delete] アイコンをクリックします。

（注） [Default] グループは削除できません。

グループ内のすべてのデバイスへのネットワーク設定の再適用

ネットワーク全体がオフラインになっている場合や、ネットワーク設定プロファイルが変更された場合など、状況によっては、デバイスグループ内の複数のデバイスに正しい設定が適用されないことがあります。これを修正するために、次の手順を使用して、ネットワーク設定プロファイルをグループ内のすべてのデバイスに再適用することができます。

1. [Administration] > [Device Groups] に移動します。
2. 再設定するグループの横にあるオプションボタンを選択し、[Edit] をクリックします。

3. ページの右上隅にある [Reapply Network Configuration] ボタンをクリックします。

デバイスグループに割り当てられた各ネットワーク設定プロファイルをグループ内のデバイスに適用するために、一連のジョブが作成されます。

デバイスのクレデンシャル

Cisco Business ダッシュボードがネットワークを完全に検出して管理するには、ネットワークデバイスで認証されるためのクレデンシャルが必要です。デバイスが最初に検出されたときに、Probe がデフォルトのユーザ名（cisco）、パスワード（cisco）、SNMP コミュニティ（public）を使用して、デバイスを認証しようとします。この試みに失敗すると通知が生成され、ユーザが有効なクレデンシャルを指定する必要があります。有効なログイン情報を提供するには、以下の手順に従ってください。

1. **[Administration]** > **[Device Credentials]** に移動します。このページの最初のテーブルには、クレデンシャルが必要な検出済みのすべてのデバイスのリストが表示されます。
2. [Username] / [Password] フィールド、[SNMP Community] フィールド、および [SNMPv3] クレデンシャル フィールドのいずれかまたはすべてに、有効なクレデンシャルを入力します。対応するフィールドの横の ✚（プラス）アイコンをクリックして、種類ごとのクレデンシャルを 3 つまで入力できます。パスワードがプレーンテキストを使用して入力されていることを確認します。

（注） [SNMPv3] クレデンシャルの場合、サポートされている認証プロトコルは None、MD5、および SHA であり、サポートされている暗号化プロトコルは None、DES、および AES です。

3. [Apply] をクリックします。Probe は各クレデンシャルを、その種類のクレデンシャルが必要な各デバイスに対してテストします。クレデンシャルが有効な場合、そのデバイスに対して後で使用するためにクレデンシャルが保存されます。
4. 必要に応じて、すべてのデバイスに有効なクレデンシャルが保存されるまで、手順 2 から 3 を繰り返します。

特定のデバイスの単一のクレデンシャルを入力するには、以下の手順に従います。

1. 検出済みデバイスのテーブル内のデバイスに対して表示されている [Edit] アイコンをクリックします。ポップアップが表示され、選択したクレデンシャルの種類に対応するクレデンシャルを入力するよう求められます。
2. ユーザ名とパスワードか、SNMP クレデンシャルをフィールドに入力します。
3. [Apply] をクリックします。適用せずにウィンドウを閉じるには、ポップアップの右上隅にある ✖ をクリックします。

[Add New Credential] セクションの下には、Probe に有効なクレデンシャルが保存されている各デバイスの ID と、クレデンシャルが最後に使用された時刻を示す表が表示されます。保存さ

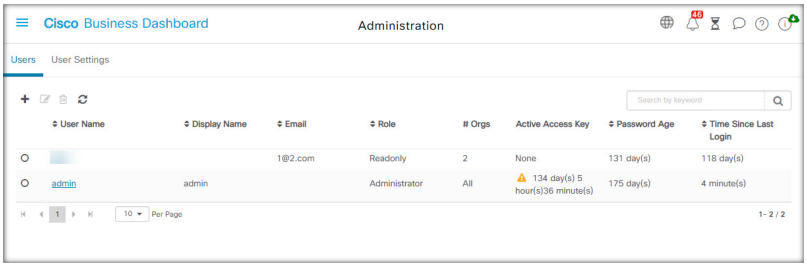
れているデバイスのクレデンシャルを表示するには、デバイスの横にある [Show Password] アイコンをクリックします。クレデンシャルを再度非表示にするには、[Hide Password] ボタンをクリックします。また、テーブルの上部にあるボタンを使用すると、すべてのデバイスのクレデンシャルを表示したり、非表示にしたりできます。不要になったクレデンシャルを削除することもできます。保存されているクレデンシャルを削除するには、以下の手順に従います。

1. **[Administration]** > **[Device Credentials]** に移動します。
2. [Saved Credentials] 表で、削除する 1 つ以上のクレデンシャルのチェックボックスをオンにします。表の一番上にあるチェックボックスをオンにして、すべてのクレデンシャルを選択することもできます。
3. [Delete Selected Credentials] をクリックします。

また、1 台のデバイスのクレデンシャルを削除するには、そのデバイスの横にある [Delete] ボタンをクリックします。

Users

[User Management] ページでは、ユーザーが Cisco Business ダッシュボードにアクセスする方法を制御したり、それらのユーザーとダッシュボードが通信する方法に影響する設定を変更したりすることができます。また、ユーザーベースのネットワーク認証を実行するときに、それらのユーザーにネットワークへのアクセスも許可するかどうかも制御できます。これは、ネットワークに対して新しいユーザーを追加または削除する必要がある場合に便利なツールです。



Cisco Business ダッシュボードには、[Dashboard Access] ドロップダウンリストを使用して利用可能なダッシュボード機能を制御する設定と、ユーザーベースのネットワークアクセス時にユーザーがネットワークにアクセスできるかどうかを制御する設定（[Network Access] チェックボックス）があります。これらの設定で使用できるオプションは次のとおりです。

- [Administrator]：管理者は、システムを保守する機能を含めて、Dashboard のすべての機能にアクセスできます。
- [Organization Administrator]：組織管理者は 1 つ以上の組織の管理に限定されていて、システムに変更を加えることはできません。
- [Operator]：オペレータは組織管理者と同様の権限を持ちますが、ユーザーを管理することはできません。

- [Readonly]：読み取り専用ユーザーは、ネットワーク情報を表示することはできますが、変更を加えることはできません。
- [No Access]：アクセス権なしのユーザーは、ダッシュボード機能を使用できません。ただし、ダッシュボードにログオンして自身のユーザープロファイルを管理することはできます。
- [Network Access]：この設定は、ユーザーベースのネットワークアクセスの使用時に、ユーザーがネットワークにアクセスできるかどうかを制御します。ダッシュボードアクセス設定が組織管理者以下に設定されている場合、ユーザーの組織リスト内の組織にのみアクセスが許可されます。

Cisco Business ダッシュボード を使用すると、ユーザがローカルユーザデータベースに対して認証されます。リリース 2.2.1 以降、ユーザは Microsoft Azure Active Directory インスタンスに対しても認証されます。

（注） ユーザーベースのネットワークアクセスの認証を実行する場合、ローカルユーザーのみがチェックされます。

Cisco Business ダッシュボード を最初にインストールすると、デフォルトの**管理者**ユーザが、ユーザ名とパスワードの両方が `cisco` に設定された状態でローカルユーザデータベースに作成されます。

（注） ユーザ設定は、**管理者**と**組織管理者**のみが管理できます。

ローカル ユーザー データベースに新しいユーザーを追加する

1. [Administration] > [Users] に移動し、[Users] タブを選択します。
2. ✚（プラス）アイコンをクリックして新しいユーザを作成します。
3. 各フィールドにユーザー名、表示名、電子メールアドレス、およびパスワードを入力し、ダッシュボードアクセスおよびネットワークアクセスの設定を指定します。また、ユーザの連絡先の詳細情報を入力することもできます。
4. [Save] をクリックします。

ユーザが**管理者**でない場合は、そのユーザを 1 つ以上の組織に追加する必要があります。これを行うには、[Organizations] タブを選択し、[+]（プラス）アイコンをクリックします。ドロップダウンリストから目的の組織を選択します。

ユーザーを変更

1. [Administration] > [Users] に移動し、[Users] タブを選択します。

2. 変更する必要があるユーザの横にあるオプションボタンを選択し、[Edit]アイコンをクリックします。
3. 必要に応じて変更を加えます。
4. [Save] をクリックします。

ユーザを新しい組織に追加するには、[Organizations] タブを選択し、[+]（プラス）アイコンをクリックします。ドロップダウンリストから目的の組織を選択します。組織から削除するには、テーブル内の組織の横にある [Delete] アイコンをクリックします。

ユーザーの削除

1. [Administration] > [Users] に移動し、[Users] タブを選択します。
2. 削除する必要があるユーザの横にあるオプションボタンを選択し、テーブルの上部にある [Delete] をクリックします。

パスワードの複雑さを変更

パスワードの複雑さの要件を有効または変更するには、次の手順に従います。

1. [Administration] > [Users] に移動し、[User Settings] タブを選択します。
2. [Authentication Source] の [Local] タブを選択し、必要に応じて [User Password Complexity] の設定を変更して、[Save] をクリックします。

（注） Azure Active Directory インスタンスに対して認証する場合、パスワードの複雑性は Active Directory で管理されます。

Azure Active Directory 認証を有効化

Cisco Business ダッシュボードは、Microsoft Azure Active Directory のインスタンスを使用したユーザ認証をサポートしています。Active Directory ユーザには、ユーザがメンバーになっている Active Directory グループに基づいてロールと組織リストが割り当てられます。

Azure Active Directory を認証ソースとして有効にするには、次の手順に従います。

1. **Azure Active Directory** で、Cisco Business ダッシュボード の新しいアプリケーション登録を作成し、**Microsoft Graph API** から User.Read および Domain.Read.All の委任権限を割り当て、**クライアントシークレット**を作成します。アプリケーション（クライアント）ID、クライアントシークレット、ディレクトリ（テナント）ID をメモします。
2. Cisco Business ダッシュボード Web GUI を開き、[Administration] > [Users] に移動します。[User Settings] タブを選択し、[Authentication Source] の [Azure AD] タブを選択します。
3. [Enable] チェックボックスをクリックします。

4. 手順 1 で収集した**クライアント ID**、**クライアントシークレット**、および**テナント ID** を所定のフィールドに入力します。
5. オプションで、ダッシュボードへのアクセスを許可するドメインのカンマ区切りリストを指定します。[Save] をクリックします。
6. [User Group Mappings] ヘッダーの下にある [+]（プラス）アイコンをクリックして、新しいグループマッピングを作成します。表示されたフィールドに Active Directory グループの**オブジェクト ID** を入力し、このグループのユーザに適用するロールと組織リストを選択します。マッピングする必要のあるすべてのグループに対してこの手順を繰り返します。

   ユーザーが複数のグループに一致する場合、最初に一致したロールと組織のマッピングが使用されます。
7. [Enable] チェックボックスの下に表示される**リダイレクト URL** をメモします。Azure Active Directory に戻り、メモした URL をアプリケーション登録用のリダイレクト URI のリストに追加します。

（注） リダイレクト URL に表示されるホストとポートは、ダッシュボードにアクセスするユーザの Web ブラウザから到達可能である必要があります。現在表示されている値に到達できない場合は、[System] > [Platform Settings] ページの [Systems Variables] タブの該当するフィールドを更新します。

ローカル認証を管理

ローカルユーザデータベースに対する認証は、デフォルトで有効になっています。ローカル認証を無効にするには、次の手順に従います。

1. Azure Active Directory に対する認証が上記のように設定されていることを確認します。Active Directory によって認証された管理者アカウントを使用してダッシュボードにログオンします。
2. [Administration] > [Users] に移動し、[User Settings] タブを選択します。[Authentication Source] で、[Local] タブを選択します。
3. [Enable] チェックボックスをオフにして、[Save] をクリックします。

ローカル認証を再度有効にするには、次の手順に従います。

1. **[Administration]** > **[Users]** に移動し、**[User Settings]** タブを選択します。[Authentication Source] で、[Local] タブを選択します。
2. [Enable] チェックボックスをオンにして、[Save] をクリックします。

すべての管理アクセスが失われた場合のアクセスを復元

Cisco Business ダッシュボード アプリケーションへの管理アクセスが失われた場合は、次の手順に従って同じアクセスを回復します。

1. SSHまたはコンソールを使用して、ホストオペレーティングシステムにログオンします。
2. **cisco-business-dashboard recoverpassword** コマンドを入力します。

コマンドを入力すると、ローカルユーザ認証が有効になり、ユーザ名が **cisco** でパスワードが **cisco** のデフォルトの管理者が復元されます。

セッションタイムアウトを変更

ユーザーセッションのアイドルタイムアウトと絶対タイムアウトを変更するには、次の手順に従います。

1. [Administration] > [Users] に移動し、[User Settings] タブを選択します。
2. 必要に応じて、[User Settings] パラメータを変更し、[Save] をクリックします。ヘルプアイコンにマウス オーバーするとこれらのパラメータの許容範囲が表示されます。

モニタリングのデフォルト値

モニタリングプロファイルを使用して、ネットワークで実行されるデバイスモニタリングを制御できます。モニタリングプロファイルは、組織レベルまたはシステムレベルで適用できます。システムレベルのモニタリングプロファイルの継承を選択した組織は、[Monitoring Defaults] ページで動作を制御します。

システム全体に適用される [Monitoring Profiles] を変更するには、以下の手順に従います。

1. **[Administration]** > **[Monitoring Defaults]** に移動します。
2. ドロップダウンを使用して、対応するタイプのデバイスに適用する適切なモニタリングプロファイルを選択します。モニタリングプロファイルの作成の詳細については、「モニタリングプロファイルの管理」を参照してください。
3. [Save] をクリックします。

実行可能なモニタリングのタイプとその設定方法の詳細については、「モニタリングプロファイル」を参照してください。組織レベルでのモニタリング設定の変更に関する詳細については、組織 （2 ページ） を参照してください。

モニタリングプロファイル

モニタリングプロファイルは、デバイスから収集されるデータと生成される通知を制御します。プロファイルは、組織内またはシステム内のさまざまなタイプのデバイスに適用できます。たとえば、デバイスによっては、場所やセキュリティ要件に応じて異なる監視要件が必要になる場合があります。プロファイル内では、**通知モニタ**と**レポートモニタ**の2種類のモニタがサポートされています。

通知モニタは、通常、デバイスの状態の変化またはしきい値を超えるパラメータに起因して、通知およびアラートを生成します。通知には、情報、警告、およびアラートの重大度レベルがあり、次のチャネルで配信されます。

- Web UI のポップアップ通知。
- 電子メール。これには、電子メール設定が正しく設定されている必要があります。詳細については、電子メール設定の管理を参照してください。
- ヘルプデスクチケット。これには、ヘルプデスクサービスを提供するアプリケーションとの統合が必要です。詳細については、統合設定の管理を参照してください。
- コラボレーションメッセージ。これには、コラボレーションアプリケーションとの統合が必要です。詳細については、統合設定の管理を参照してください。

（注） モニタリングプロファイルを設定して、チケットまたはコラボレーションメッセージの平均レートが 1 時間あたり 60 を超えないようにすることをお勧めします。外部アプリケーションと通信する場合、これを超えるレートが持続すると、API の輻輳とイベントの損失が発生する可能性があります。

アクティブな通知は [Notification Center] にも表示され、デバイス情報ビューにも表示されます。通知の変更も [Event Log] に記録されます。

レポートモニタは、監視ダッシュボードのワイヤレスレポートおよびトラフィックグラフで使用されるデータを収集します。

複数のモニタリングプロファイルを作成し、システムレベルで、または組織ごとに、異なるデバイスタイプに異なるプロファイルを割り当てることができます。プロファイルへのテンプレートの割り当てに関する詳細については、組織 （2 ページ） と モニタリングのデフォルト値 （11 ページ） を参照してください。

新しいモニタリングプロファイルを追加

1. **[Administration]** > **[Monitoring Profiles]** に移動します。
2. [+]（プラス）アイコンをクリックして新しいプロファイルを作成します。
3. プロファイルの名前と、プロファイルを関連付ける組織を指定します。ここで [All Organizations] を指定して、プロファイルを任意の組織で使用できるようにしたり、システムレベルのデフォルトとして使用したりすることもできます。
4. プロファイルの説明と、通知を受信する電子メールアドレスのカンマ区切りリストを指定することもできます。
5. [Save] をクリックします。
6. 画面が更新され、さまざまな通知モニタとレポートモニタが表示されます。用意されているコントロールを使用して、個々のモニターを有効または無効にすることができます。

7. 通知モニターには、[Edit] アイコンをクリックして変更できる追加の設定があります。設定はモニタによって異なりますが、生成される通知タイプ、通知のシビラティ（重大度）、通知をトリガーするしきい値が含まれます。

既存のモニタリングプロファイルをコピー

既存のモニタリングプロファイルをコピーするには、以下の手順に従います。

1. [Administration] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスを選択し、[Save As] アイコンをクリックします。
3. 必要に応じてプロファイル名、説明、組織、電子メールアドレスを更新してから、[Save] をクリックします。
4. 必要に応じて、通知モニタとレポートモニタを変更します。[Reset to defaults] ボタンをクリックすると、モニター設定をデフォルトに戻すことができます。

モニタリングプロファイルを変更

既存のモニタリングプロファイルを変更するには、以下の手順に従います。

1. [Administration] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスを選択し、[Edit] アイコンをクリックします。
3. 必要に応じてプロファイル設定と電子メールアドレスを更新してから、[Save] をクリックします。
4. 必要に応じて、通知モニタとレポートモニタを変更します。[Reset to defaults] ボタンをクリックすると、モニター設定をデフォルトに戻すことができます。

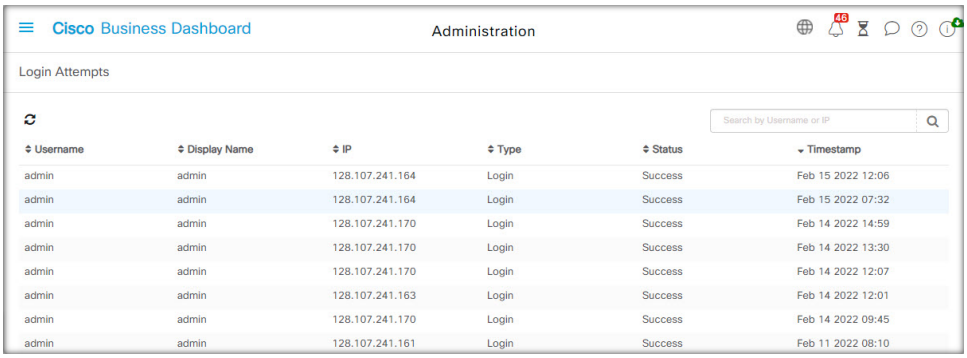
モニタリングプロファイルを削除

1. [Administration] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスをオンにして、[Delete] アイコンをクリックします。

（注） プロファイルが組織レベルのモニタリングプロファイルとして使用されている場合は、対応する組織とデバイスタイプがシステムレベルの設定を継承するように更新されます。システムレベルのモニタリングプロファイルとして使用されているプロファイルは削除できません。プロファイルを削除する前に、そのプロファイルを [Administration] > [Monitoring Defaults] ページから削除します。

ログイン試行の表示

Cisco Business ダッシュボードは、システムへのログインとシステムからのログアウトが成功したか失敗したかを記録します。



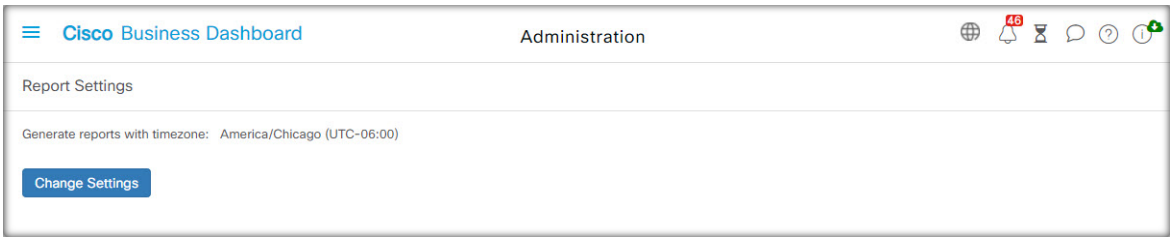
ログを表示するには、[Administration] > [Login Attempts] に移動します。テーブルに表示される情報は次のとおりです。

フィールド	説明
Username	イベントに関連付けられているユーザ名。
Display Name	ユーザの表示名。
IP	ユーザのログイン元であるデバイスの IP アドレス。
Type	イベントのタイプ。次の項目があります。 • LOGIN • LOGOUT
Status	試行が成功したか失敗したかを示します。
Timestamp	イベントが発生した日時。

テーブルの上の検索ボックスを使用すると、特定のユーザまたは IP アドレスに一致するエントリのみを表示できます。

レポート設定の管理

[Report Settings] ページを使用し、レポートを生成するタイムゾーンを設定できます。



レポート期間の開始時間と終了時間は、設定したタイムゾーンの現地時間になります。

翻訳について
このドキュメントは、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。