システム

この章は、次の項で構成されています。

システムについて

Cisco Business ダッシュボード の [System] オプションを使用すると、プラットフォームの動作を管理できます。

このセクションは、次のページに分かれています。

ページ名	ページ機能
ライセンス（License）	Dashboard のソフトウェアライセンスを管理します。
証明書（Certificate）	Dashboard でセキュリティ証明書を管理します。
電子メール設定（Email Settings）	電子メールを設定し、設定を管理します。
API の使用状況（API Usage）	Cisco Business ダッシュボード API の使用状況を監視します。

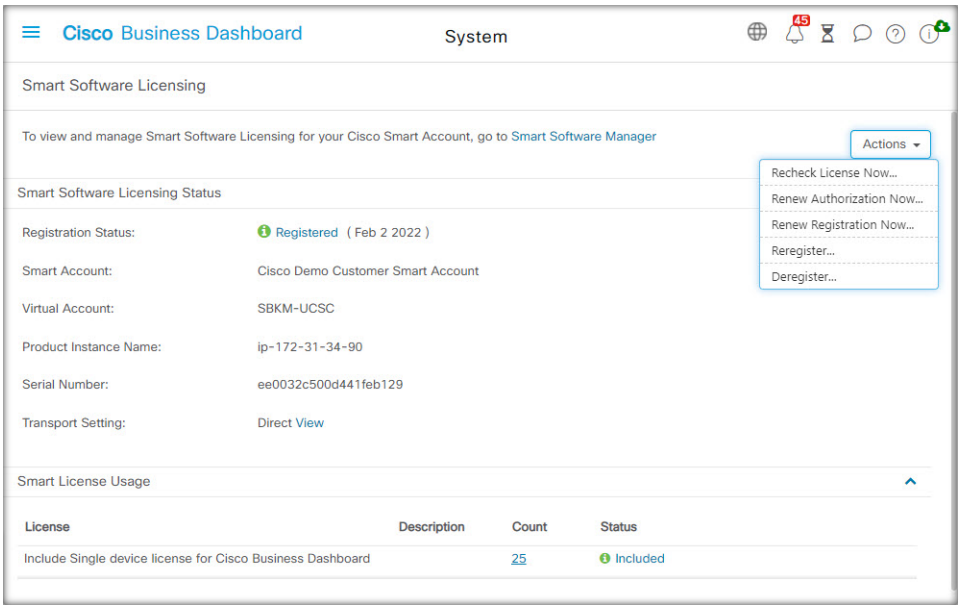
ページ名	ページ機能
バックアップ（**Backup**）	Dashboard 用の設定とその他のデータをバックアップします。
Restore（復元）	Dashboard 用の設定とその他のデータを復元します。
プラットフォームの設定（**Platform Settings**）	Dashboard のネットワーク設定を管理します。
プライバシー設定（**Privacy Settings**）	シスコと共有できるデータを制御します。
ログ設定（**Log Settings**）	Dashboard のログ設定を変更します。
ローカルプローブ（**Local Probe**）	Dashboard にホストされた Probe を管理します。
統合設定（**Integration Settings**）	Cisco Business Dashboard と外部アプリケーションの統合を管理します。

（注） これらのページは、**管理者**のみが使用できます。

ライセンスの管理

（注） このページは、Cisco Business ダッシュボード for AWS の従量制課金バージョンには表示されません。

[License]ページでは、ネットワークで必要なライセンスの数とタイプを確認すること、および **Dashboard** を Cisco Smart Licensing システムに接続することができます。デバイス数が 25 以下の場合、追加のライセンスは必要ありません。このページには、次の 2 つの情報パネルがあります。



- **スマート ソフトウェア ライセンシングのステータス**

  このパネルには、スマート ライセンス クライアントの登録状態と使用中のスマートアカウントに関する情報が表示されます。

- **スマート ライセンスの使用状況**

  このパネルには、ネットワークの現在の状態に基づいて必要なライセンスの数と種類が一覧表示されます。この情報は、ネットワークが変更されると自動的に更新されます。また、Dashboard でスマートアカウントから要求されるライセンスの数が更新されます。[Status] フィールドにより、必要な数のライセンスが正常に取得されたかどうかが示されます。

また、このページには、スマートアカウントに対して Dashboard を登録および登録解除するためのコントロールも含まれます。

Dashboard がネットワークを管理するための十分なライセンスを取得できない場合、Dashboard は評価モードで実行され、Dashboard のユーザインターフェイスのヘッダーにメッセージが表示されます。評価モードで実行する場合、状況を改善するための猶予期間は 90 日です。90 日以内に問題が解決されない場合、問題が解決されるまで Dashboard の一部の機能が制限されます。問題を解決するには、追加ライセンスを取得するか、管理対象デバイスの数を減らす必要があります。

スマートアカウントへの Dashboard の登録

Dashboard をスマートアカウントに登録するには、次の手順に従います。

1. *https://software.cisco.com* にあるスマート アカウントにログオンします。

   [License] セクションの下にある [Smart Software Licensing] リンクを選択します。

2. [Inventory] ページを選択し、必要に応じて、選択した仮想アカウントをデフォルトから変更します。
3. [General] タブをクリックします。
4. [New Token…] ボタンをクリックして、新しい**製品インスタンス登録トークン**を作成します。オプションで、説明を追加し、[Expire After] の時間を変更します。
5. [Create Token] をクリックします。
6. トークンの右にある [Actions] ドロップダウンから [Copy] を選択して、新しく作成したトークンをクリップボードにコピーします。
7. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
8. [Register] ボタンをクリックし、表示されるフィールドにトークンを貼り付けます。
9. [OK] をクリックします。

Dashboard が Cisco Smart Licensing に登録され、管理対象ネットワークデバイスの数に見合う十分なライセンスが要求されます。使用可能なライセンスが不十分である場合、ユーザインターフェイスにメッセージが表示され、十分なライセンスを取得するための 90 日の期間が与えられます。この期間が経過すると、システムの機能が制限されます。

スマートアカウントから Dashboard を削除

スマートアカウントから Dashboard を削除し、割り当てられたライセンスをプールに戻すには、次の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Deregister…] を選択します。ポップアップで [Deregister] をクリックして確定します。

ライセンスを今すぐ確認

Cisco Business ダッシュボード は、毎日チェックを実行して、ネットワークに対して使用できる十分なライセンスがその時点で存在するかどうか確認し、必要なライセンスの数が減少している場合にはただちに更新を行います。ただし、必要なライセンスの数が増加している場合、またはプールに対してライセンスが追加または削除された場合、Dashboard が更新されるまでに最大で 1 日かかる場合があります。Dashboard にライセンス割り当てをすぐに更新させるには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上のドロップダウンリストから [ReCheck License Now…] を選択します。 Cisco Business ダッシュボード は Cisco Smart Licensing にただちに問い合わせて、Dashboard の稼働に使用できる十分なライセンスがあるかどうか確認します。

認証を今すぐ更新

[Renew Registration Now] アクションを使用すると、Dashboardは Cisco Smart Licensing との通信を認証するために使用される証明書を更新します。通常、これは、拡張された通信の停止を回避する場合に、シスコ サポートの要求でのみ必要になります。登録を更新するには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Renew Authorization Now…] を選択します。

登録を今すぐ更新

[Renew Registration Now] アクションを使用すると、Manager は Cisco Smart Licensing との通信を認証するために使用される証明書を更新します。通常、これは、拡張された通信の停止を回避する場合に、シスコ サポートの要求でのみ必要になります。登録を更新するには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Renew Registration Now…] を選択します。

異なるアカウントへの Dashboard の移動

Dashboard を再登録すると、一方の仮想アカウントから別の仮想アカウントに Dashboard を移動できます。アカウント間で Dashboard を移動するには、以下の手順に従います。

1. Cisco Business ダッシュボード ユーザインターフェイスに移動し、**[System]** > **[License]** を選択します。
2. 右上にあるドロップダウンリストから [Reregister...] を選択します。
3. 表示されるボックスに新しい登録トークンを入力します。Dashboard が別のアカウントに現在登録されている場合、[Reregister this product instance if it is already registered] チェックボックスが選択されていることを確認し、[OK] をクリックします。

証明書の管理

Cisco Business ダッシュボード のインストール時に、サーバとの Web 通信その他の通信を保護するために自己署名証明書が生成されます。この証明書は、信頼される認証局（CA）が署名した証明書に置き換えることができます。

これには、次のようないくつかの方法があります。

- Cisco Business Dashboard は、Let's Encrypt 認証局からの証明書の自動発行および更新をサポートしています。

- 署名のために、希望する認証局に証明書署名要求（CSR）を提供することができます。Cisco Business Dashboard によって CSR が生成されます。
- ダッシュボードとは独立して、認証局で証明書および対応する秘密キーを生成させることもできます。その際、証明書チェーンと秘密キーを PKCS#12 形式のファイルに結合してからダッシュボードにアップロードする必要があります。

これらの各オプションの詳細と、現在の証明書を表示する手順および自己署名証明書を再生成する手順については、以下のセクションを参照してください。

Let's Encrypt からの証明書の自動インストール

リリース 2.2.1 以降、Cisco Business Dashboard は、**Let's Encrypt Certificate Authority**（https://letsencrypt.org/ja/）からドメイン検証済み証明書を自動的に取得して更新できるようになり、リリース 2.5.0 では、これらの証明書を管理ページから管理することができます。

重要 登録済みの完全修飾ドメイン名と、パブリック IP アドレスを指す DNS レコードが必要です。詳細については、プラットフォーム設定の管理 （14 ページ）を参照してください。

管理 GUI を使用して Let’s Encrypt 証明書をインストールするには、次の手順を実行します。

1. [System] > [Certificate] に移動し、[Update Certificate] タブを選択します。
2. [Let’s Encrypt Certificate] オプションボタンを選択します。
3. チェックボックスをオンにすると、Let's Encrypt 証明書の使用が有効になります。
4. 提示されたフィールドに 1 つ以上の完全修飾ドメイン名を入力します。名前はドメインネームシステム（DNS）で定義され、Cisco Business Dashboard サーバーのアドレスに解決される必要があります。
5. 緊急の更新およびセキュリティ通知に使用する電子メールアドレスを指定します。
6. 提示されたリンクを使用して Let's Encrypt 利用規約を確認し、チェックボックスをオンにして利用規約に同意します。
7. 必要に応じて、電子メールアドレスを電子フロンティア財団（https://www.eff.org）と共有するためのチェックボックスをオンにします。
8. [Get Certificate] ボタンをクリックします。

ダッシュボードが Let's Encrypt 認証局に接続され、HTTP 検証方法を使用して証明書が取得されます。ページが更新され、証明書の詳細が有効期限とともに表示されます。証明書は、有効期限の約 30 日前に自動的に更新されます。

任意の時点で証明書を更新する必要がある場合は、次の手順に従います。

1. [System] > [Certificate] に移動し、[Update Certificate] タブを選択します。
2. [Let’s Encrypt Certificate] オプションボタンを選択します。

3. 提示されているチェックボックスとフィールドを使用して、証明書に適用する名前を更新します。

   または、画面の下部で連絡先の詳細を更新できます。

4. [Get Certificate] ボタンをクリックします。

ページのフィールドを変更せず、[Force Renewal] ボタンをクリックすることで、通常の更新時間の前に証明書を強制的に再生成することもできます。

コマンドラインを使用して Let's Encrypt 証明書をインストールするには、次の手順を実行します。

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 letsencrypt** コマンドを実行し、**-d** オプションを使用して 1 つ以上の完全修飾ホスト名を指定します。（たとえば、**cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com** のように指定します。）コマンドに表示されるすべての名前は、ダッシュボードサーバの IP アドレスに解決される必要があります。
3. プロンプトに従って証明書を発行し、ダッシュボードアプリケーションに適用します。証明書は、有効期限が近づくとダッシュボードによって自動的に更新されます。

（注） **Let’s Encrypt** サービスは、ダッシュボード Web サーバに接続してホスト名の所有権を確認する必要があります。これを可能にするには、ダッシュボード Web サーバーにインターネットからアクセスできる必要があります。ダッシュボードアプリケーションへのアクセスを許可された IP アドレスのみに制限する方法の詳細については、プラットフォーム設定の管理 （14 ページ） を参照してください。

証明書署名要求（CSR）の生成

1. [System] > [Certificate] に移動し、[CSR] タブを選択します。
2. 表示されるフォームにあるフィールドに適切な値を入力します。これらの値は、CSR を生成するために使用され、CA から受信する署名証明書に組み込まれます。
3. [Create] をクリックします。これにより、CSR が PC に自動的にダウンロードされます。また、CSR ラベルの横にある [Download] をクリックすることで、後日 CSR をダウンロードすることもできます。
4. 必要に応じて手順 2 に戻ることで、CSR を変更できます。

新しい証明書をアップロード

管理 GUI を使用して新しい証明書をアップロードするには、以下の手順に従います。

1. [System] > [Certificate] に移動し、[Update Certificate] タブを選択します。

2. [Upload Cert] オプション ボタンを選択します。証明書を含むファイルはターゲット領域で廃棄してかまいません。また、ターゲット領域をクリックすると、ファイルシステムをブラウズできます。ファイルは PEM 形式でなければなりません。

   また、代わりに [Upload PKCS12] オプションを選択することで、PKCS#12 形式で証明書と関連するプライベート キーをアップロードできます。用意されているフィールドに、ファイルをロック解除するためのパスワードを指定する必要があります。

3. [Upload] をクリックしてファイルをアップロードし、現在の証明書を置き換えます。

コマンドラインを使用して新しい証明書をアップロードするには、次の手順を実行します。

1. SCP などを使用して、証明書と秘密キーファイルを Cisco Business Dashboard ファイルシステムにコピーします。秘密キーは機密情報であるため、これらのファイルへのアクセスは、承認された担当者のみに制限してください。
2. コンソールまたは SSH を使用して、オペレーティングシステムにログオンします。
3. コマンド **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>** を使用して、ダッシュボードアプリケーションに証明書を適用します。証明書と秘密キーがダッシュボードアプリケーションにロードされ、現在の証明書が新しいものに置き換えられます。このコマンドとそのオプションの詳細については、**cisco-business-dashboard importcert -h** と入力してください。

（注） 一部のブラウザでは既知の認証局によって署名された証明書に証明書の警告が生成される場合がありますが、他のブラウザでは警告なしに証明書が受け入れられる場合もあります。ネットワーク プラグアンドプレイ クライアントも証明書の受け入れに失敗する場合があります。これは、認証局がブラウザまたはPnPクライアントの信頼された認証局ストアに含まれていない中間証明書を使用して証明書に署名しているためです。このような状況では、認証局は、Dashboard にアップロードする前にサーバ証明書と連結させる必要のある一連の証明書を提供します。

アップロード中、Dashboard は、チェーンから重複または不要な証明書を削除し、正しい順序で組み立てることを試みます。アップロード後に [Current Certificate] タブを選択して、証明書チェーンが完全で正しい形式であることを確認してください。

自己署名証明書を再生成

自己署名証明書を再生成するには、以下の手順に従います。

1. [System] > [Certificate] に移動し、[Update Certificate] タブを選択します。
2. [Renew Self-Signed Cert] をクリックします。表示されるフォームにあるフィールドに適切な値を入力します。これらの値は、証明書の作成に使用されます。
3. [Save] をクリックします。

現在の証明書を表示

現在の証明書を表示するには、次の手順に従います。

1. [System] > [Certificate] に移動し、[Current Certificate] タブを選択します。
2. Dashboard の信頼チェーン内の各証明書は、そのタイプ、サブジェクト、および有効期限とともに、画面上部のテーブルに示されます。自己署名証明書を使用する Dashboard の場合、テーブルには 1 つのエントリのみが表示されますが、CA 署名証明書を使用する Dashboard の場合、テーブルには複数のエントリが含まれることがあります。
3. テーブルの行をクリックすると、対応する証明書の詳細情報が下のボックスに表示されます。
4. [Actions] 列のアイコンを使用して、チェーン内のルート証明書を下に移動させたり、クリップボードにコピーすることができます。証明書が自己署名されている場合またはプライベート CA によって署名されている場合に Dashboard に接続するようにデバイスを設定するときに、ルート証明書が必要になることがあります。

現在の証明書チェーンのダウンロード

現在の証明書チェーンのコピーをダウンロードするには、次の手順に従います。

1. [System] > [Certificate] に移動し、[Current Certificate] タブを選択します。
2. ページ下部にある [Download Certificate Chain] ボタンをクリックします。証明書チェーンがブラウザにより PEM 形式でダウンロードされます。

Let's Encrypt からの証明書の自動インストール

リリース 2.2.1 以降、Cisco Business Dashboard は、**Let's Encrypt Certificate Authority**（https://letsencrypt.org/ja/）からドメイン検証済み証明書を自動的に取得して更新できるようになり、リリース 2.5.0 では、これらの証明書を管理ページから管理することができます。

重要 登録済みの完全修飾ドメイン名と、パブリック IP アドレスを指す DNS レコードが必要です。詳細については、プラットフォーム設定の管理 （14 ページ）を参照してください。

管理 GUI を使用して Let’s Encrypt 証明書をインストールするには、次の手順を実行します。

1. [System] > [Certificate] に移動し、[Update Certificate] タブを選択します。
2. [Let’s Encrypt Certificate] オプションボタンを選択します。
3. チェックボックスをオンにすると、Let's Encrypt 証明書の使用が有効になります。
4. 提示されたフィールドに 1 つ以上の完全修飾ドメイン名を入力します。名前はドメインネームシステム（DNS）で定義され、Cisco Business Dashboard サーバーのアドレスに解決される必要があります。
5. 緊急の更新およびセキュリティ通知に使用する電子メールアドレスを指定します。

6. 提示されたリンクを使用して Let's Encrypt 利用規約を確認し、チェックボックスをオンにして利用規約に同意します。
7. 必要に応じて、電子メールアドレスを電子フロンティア財団（https://www.eff.org）と共有するためのチェックボックスをオンにします。
8. [Get Certificate] ボタンをクリックします。

ダッシュボードが Let's Encrypt 認証局に接続され、HTTP 検証方法を使用して証明書が取得されます。ページが更新され、証明書の詳細が有効期限とともに表示されます。証明書は、有効期限の約 30 日前に自動的に更新されます。

任意の時点で証明書を更新する必要がある場合は、次の手順に従います。

1. [System] > [Certificate] に移動し、[Update Certificate] タブを選択します。
2. [Let’s Encrypt Certificate] オプションボタンを選択します。
3. 提示されているチェックボックスとフィールドを使用して、証明書に適用する名前を更新します。

   または、画面の下部で連絡先の詳細を更新できます。
4. [Get Certificate] ボタンをクリックします。

ページのフィールドを変更せず、[Force Renewal] ボタンをクリックすることで、通常の更新時間の前に証明書を強制的に再生成することもできます。

コマンドラインを使用して Let's Encrypt 証明書をインストールするには、次の手順を実行します。

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 letsencrypt** コマンドを実行し、**-d** オプションを使用して 1 つ以上の完全修飾ホスト名を指定します。（たとえば、**cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com** のように指定します。）コマンドに表示されるすべての名前は、ダッシュボードサーバの IP アドレスに解決される必要があります。
3. プロンプトに従って証明書を発行し、ダッシュボードアプリケーションに適用します。証明書は、有効期限が近づくとダッシュボードによって自動的に更新されます。

（注） **Let’s Encrypt** サービスは、ダッシュボード Web サーバに接続してホスト名の所有権を確認する必要があります。これを可能にするには、ダッシュボード Web サーバーにインターネットからアクセスできる必要があります。ダッシュボードアプリケーションへのアクセスを許可された IP アドレスのみに制限する方法の詳細については、プラットフォーム設定の管理 （14 ページ） を参照してください。

電子メール設定の管理

[Email Settings] ページでは、電子メールが Cisco Business ダッシュボード によって送信される方法を制御できます。

このページにアクセスして、以下のパラメータを設定してください。

フィールド	説明
SMTP Server	使用する SMTP サーバのドメイン名または IP アドレス。
SMTP Port	メールを送信するために使用される TCP ポート。
Email Encryption	使用する暗号化方式には、次のものが含まれます。 • なし • TLS • SSL
Authentication	電子メール認証を有効または無効にします。
Username	認証が有効な場合に提示するユーザ名。
Password	認証が有効な場合に提示するパスワード。
From Email Address	メッセージの送信元の電子メール アドレス。

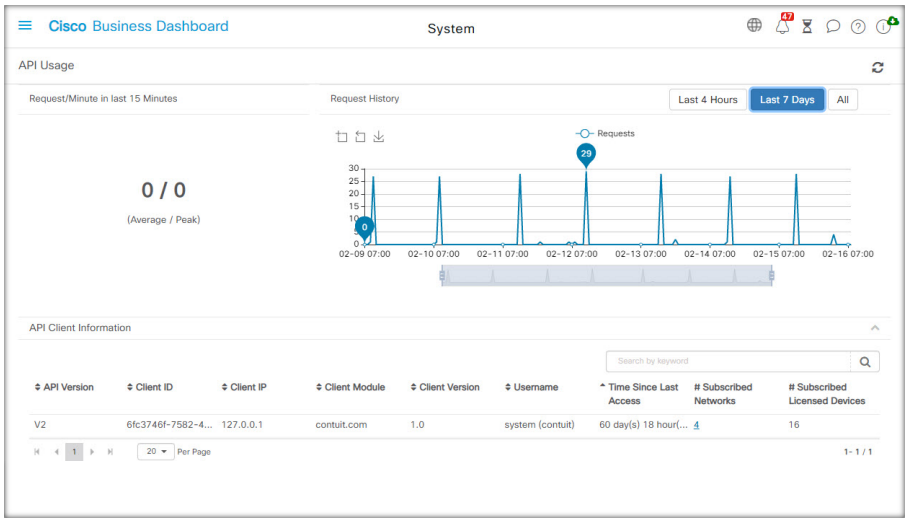
設定をテストするには、[Test Connectivity] をクリックします。これにより、ターゲットの電子メールアドレスの入力が要求され、指定されたアドレスにテスト用の電子メールが生成されます。

API 使用状況の表示

[API Usage] ページには、Cisco Business ダッシュボード と統合されているすべての外部アプリケーションに関する情報が表示されます。このレポートは次の 3 つのセクションに分かれています。

- [15-minute Request Monitor]：過去 15 分間の平均要求レートとピーク要求レートを表示します。
- [Request History] グラフ：時間の経過に伴う要求アクティビティのグラフを表示します。過去 4 時間、過去 7 日間、または使用可能なすべての情報の期間を選択できます。次に、グラフの下にあるスライダを使用して、グラフのフォーカスを特定の対象期間に絞り込むことができます。

- [API Client Information] テーブル：API を 1 回以上使用したすべてのクライアントのリストが表示されます。次の表で、[API Client Information] テーブルに表示される情報について説明します。



フィールド	説明
API Version	API にアクセスするときにクライアントが使用するバージョン。
Client ID	クライアント アプリケーションの特定のインスタンスの識別子。
Client IP	このクライアントに関連付けられている IP アドレス。また、API バージョンが v1 で通知が要求されたときに、Dashboard がイベント通知をポストする必要があるコールバック URL も表示されます。
Client Module	このクライアントに関連付けられているアプリケーションのタイプ。
Client Version	このクライアントに関連付けられているアプリケーションのバージョン。
Username	v1 API を使用するクライアントの場合、このフィールドには、Dashboard への認証時にアプリケーションによって提示されたユーザ名が表示されます。v2 API を使用するクライアントの場合、このフィールドには、クライアントが使用する**アクセス キー ID** と、キーが関連付けられているユーザ名が表示されます。
Time Since Last Access	このクライアントからの最後のアクティビティ以降の時間。
# Subscribed Networks	アプリケーションがイベント通知を要求したネットワークの数。この数値は、クリックすると、このクライアントの登録済みネットワーク テーブルを表示するリンクです。次に、登録済みネットワークのテーブルについて説明します。

フィールド	説明
# Subscribed Licensed Devices	このクライアントにイベント通知を送信する管理対象デバイスの数。

クライアントが通知を要求したネットワークに関する情報を表示するには、[API Client Information] テーブルにあるクライアントの [# Subscribed Networks] リンクをクリックします。クライアントが通知を要求したネットワークのリストが含まれているクライアントの [Subscribed Networks] テーブルが表示されます。

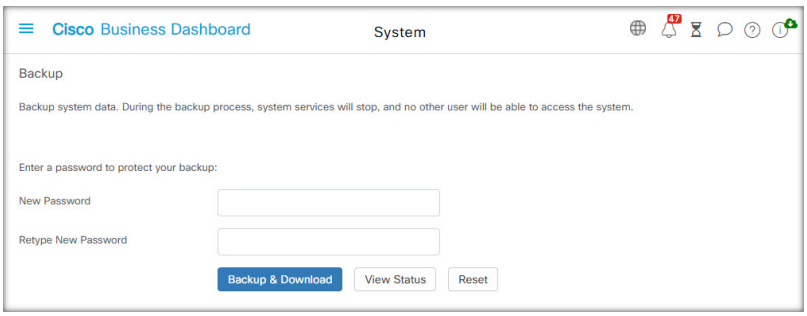
フィールド	説明
Network	クライアントによって監視されているネットワークの名前。
# Subscribed Licensed Devices	イベント通知を送信するこのネットワーク内の管理対象デバイスの数。

Dashboard 設定のバックアップと復元

ディザスタリカバリのために、または Dashboard を新しいホストに容易に移行するために、Cisco Business ダッシュボードが使用する設定などのデータをバックアップできます。機密データを保護するため、バックアップはパスワードで暗号化されます。

Cisco Business ダッシュボードバックアップファイルは、バックアップされたシステムと同じバージョンを実行しているシステム、または最大1つの新しいマイナーリリースを実行しているシステムに復元できます。たとえば、バージョン 2.2.0 を実行しているシステムから作成されたバックアップは、2.3.1 を実行しているシステムには復元できますが、2.4.0 を実行しているシステムには復元できません。

バックアップを実行するには、以下の手順に従います。

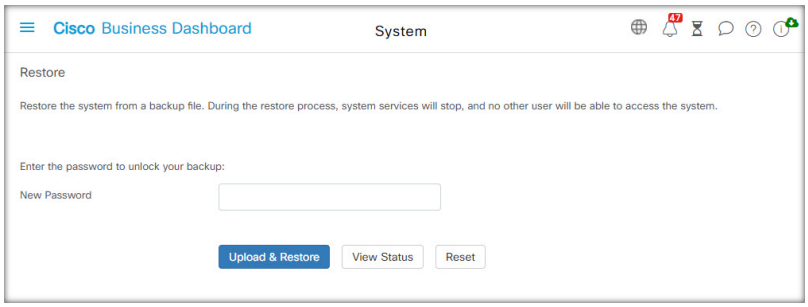


1. **[System]** > **[Backup]** に移動します。
2. バックアップを暗号化するためのパスワードを、[Password] および [Confirm Password] フィールドに入力します。
3. [Backup & Download] をクリックします。ポップアップウィンドウが表示され、バックアップの進行状況が表示されます。大規模なシステムでは、バックアップの完了までに時間が

かかる可能性があるため、進行状況メーターを非表示にし、後で [View Status] アイコンを使用して再度表示こともできます。

完了すると、バックアップ ファイルが PC にダウンロードされます。

構成のバックアップを Dashboard に復元するには、以下の手順に従います。



1. **[System]** > **[Restore]** に移動します。
2. バックアップを暗号化するために使用したパスワードを、[Restore] フィールドに入力します。
3. [Upload & Restore] をクリックして続行します。ポップアップが表示され、PC からバックアップファイルをアップロードできるようになります。用意されたターゲット領域にバックアップファイルをドラッグアンドドロップするか、ターゲット領域をクリックして、PC のファイルシステム内のファイルを指定できます。[Restore] をクリックして続行します。

ダッシュボードのバージョンが 2.5.0 以降の場合、復元プロセスが完了するとアプリケーションが再起動します。

プラットフォーム設定の管理

[Platform Settings] ページでは、オペレーティングシステムに直接アクセスせずに主要なシステム設定を変更できます。Cisco Business ダッシュボードによってサポートされるプラットフォームにはさまざまな種類があるため、すべてのプラットフォームですべての設定を使用できるわけではありません。

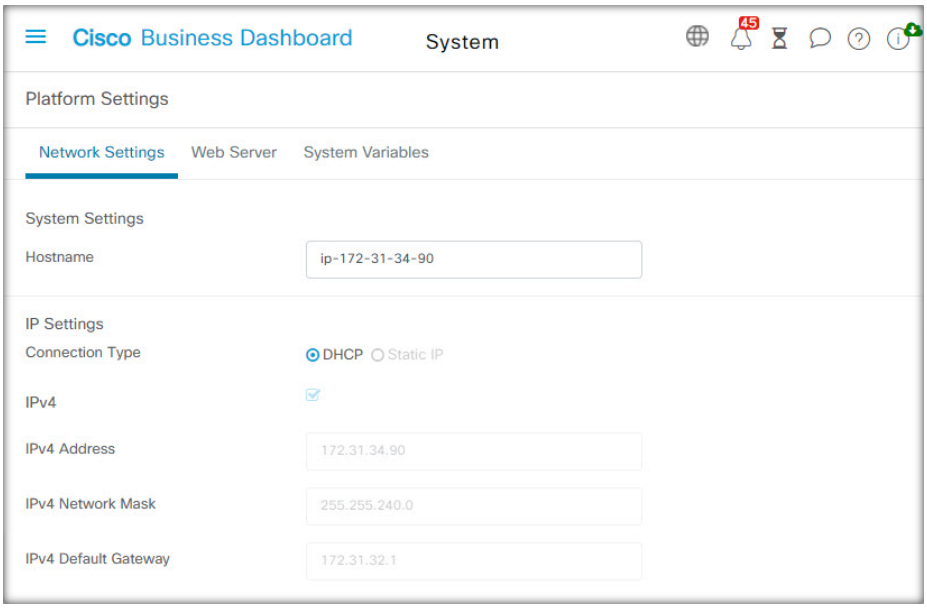
プラットフォーム設定は 3 つのグループに分かれています

- ネットワーク設定
- ウェブ サーバ
- システム変数

以下のセクションでは、各タブで実行可能な設定について説明します。

ホスト名の変更（[Network Settings] タブ）

ホスト名は、オペレーティングシステムがシステムを特定するために使用する名前で、Bonjour アドバタイズメントを生成する際、Cisco Business ダッシュボード が Dashboard を特定するために使用されます。

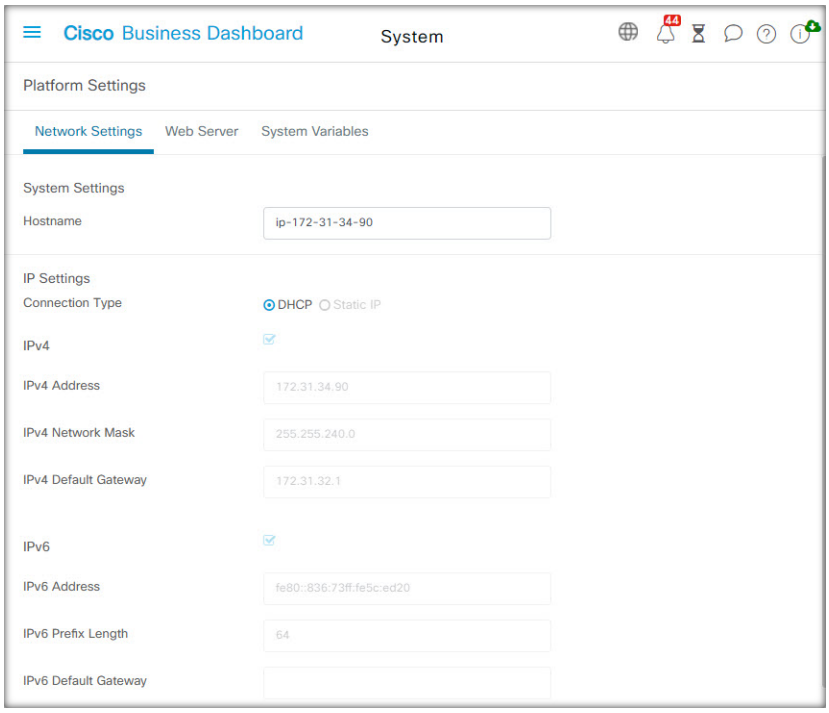


Dashboard のホスト名を変更するには、以下の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Network Settings] タブを選択します。
2. 表示されたフィールドで、Dashboard のホスト名を指定します。
3. [Save] をクリックします。

ネットワーク設定の変更（[Network Settings] タブ）

（注） これは、AWS または Azure 用の Cisco Business ダッシュボード には適用されません。ネットワーク構成を変更するには、AWS インスタンスの場合は AWS の EC2 コンソールを使用し、Azure インスタンスの場合は Azure ポータルを使用します。

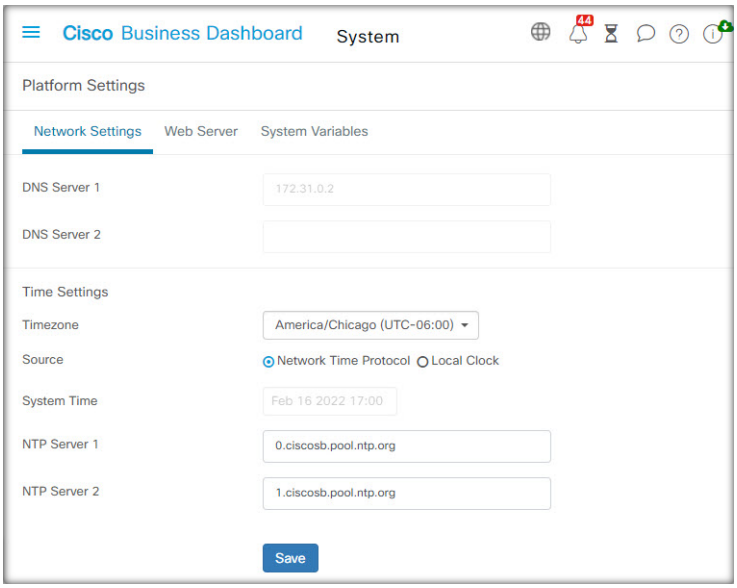


Dashboard のネットワーク構成を変更するには、以下の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Network Settings] タブを選択します。
2. IP アドレスの割り当て方法を選択します。指定可能なオプションは、[DHCP]（デフォルト）と [Static IP] です。[Static IP] オプションを選択する場合は、アドレス、サブネット マスク、デフォルト ゲートウェイ、DNS サーバを適切なフィールドに指定します。
3. [Save] をクリックします。

時刻設定の変更（[Network Settings] タブ）

[Time Settings] では Dashboard のシステムクロックを管理します。システムクロックを調整するには、以下の手順に従います。



1. **[System]** > **[System Platform Settings]**に移動し、[Network Settings] タブを選択します。
2. Dashboard に適切なタイムゾーンを選択します。
3. 時刻同期の方法を選択します。指定可能なオプションは、[NTP]（デフォルト）と [ローカル クロック] です。[NTP] オプションを選択した場合は、同期に使用する NTP サーバを必要に応じて変更します。

   [Local Clock] が選択されている場合、表示されているコントロールを使用して手動で日付と時刻を調整できます。また、[Clock] をクリックして、PC の時刻と同期させます。
4. [Save] をクリックします。

（注） 仮想マシンがローカル クロックとホスト マシンと同期させるように設定されている場合、[Platform Settings] ページから行ったローカル クロックの変更は、ハイパーバイザにより上書きされます。

使用中のハイパーバイザが VirtualBox で、VirtualBox Guest Additions が VM にインストールされている場合、NTP サービス（timesyncd）は動作しません。

ポート設定の変更（[Web Server] タブ）

[Port Settings] では、Dashboard のユーザインターフェイスがホストされる TCP ポートを管理します。デフォルトの Web サーバーポートを変更するには、以下の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Web Server] タブを選択します。
2. HTTP および HTTPS プロトコル用に Web サーバが使用するポートを変更します。

3. Cisco Business Dashboard を介してネットワークデバイスへのリモートアクセスを提供するために使用されるポートを変更します。
4. [Save] をクリックします。

Dashboard へのアクセスの制限（[Web Server] タブ）

[Access Control] 設定を使用して、Dashboard にアクセスできる IP アドレスを制限できます。Dashboard GUI、Dashboard API、およびプローブと管理対象デバイスからの接続に異なる IP 範囲を指定できます。

Dashboard へのアクセスを制限するには、次の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[Web Server] タブを選択します。
2. 表示されたフィールドにネットワークプレフィックスおよびマスクを入力します。いずれかのセクションに複数のプレフィックスが必要な場合は、[+]（プラス）アイコンをクリックしてエントリを追加します。同様に、ごみ箱アイコンをクリックして既存のエントリを削除することもできます。
3. [Save] をクリックします。

システム変数の管理（[System Variables] タブ）

Cisco Business ダッシュボード 設定テンプレートやその他のタスクを生成するときに、システム変数を使用して、Dashboard に関連した特定のパラメータを入力します。一部のシステム変数は Dashboard によって自動的に決定されますが、ユーザ入力を必要とする変数もあります。特に、Dashboard が Web プロキシまたは NAT ゲートウェイの背後に展開されている場合、管理者は Dashboard の外部アドレッシング情報を提供する必要があります。

Dashboard の外部アドレス情報を更新するには、次の手順に従います。

1. **[System]** > **[System Platform Settings]**に移動し、[System Variables] タブを選択します。
2. 必要に応じて、[External System Settings] パラメータに IP アドレスとポート情報を入力します。空白のままにすると、Dashboard は、対応するシステム変数のプラットフォームアドレスとポート情報を使用します。
3. [Save] をクリックします。

プライバシーの管理

Cisco Business ダッシュボード の一部の機能には、シスコがホストするオンライン サービスを使用する必要があります。そのため、特定の情報をシスコと共有することになります。具体的には、次のようなサービスがあります。

- **Lifecycle Reporting**：この機能には、Cisco Business ダッシュボード に **ライフサイクルレポート、サポート終了レポート、およびメンテナンスレポート**の生成が含まれています。ライフサイクルレポートはデフォルトで有効になっています。

- **Software Updates**：ネットワークデバイスのソフトウェア更新プログラムの可用性の通知と、それらの更新プログラムを自動的に適用する機能。ソフトウェアの更新はデフォルトで有効になっています。

これらの機能はすべてシスコのプライバシーポリシーの対象であり、いつでも有効または無効にすることができます。[Privacy Settings] ページは、Dashboard の初期セットアップ時に表示され、ネットワークデータが収集される前に、デフォルトで有効になっているどの機能も無効にすることができます。これらの機能と共有される情報の詳細については、以下を参照してください。

Lifecycle Reporting

Cisco Business ダッシュボードは、ネットワーク内の各シスコ デバイスのライフサイクル状態に関する情報を提供します。これを実行するには、Dashboard が各シスコデバイスの製品 ID、シリアル番号、ハードウェアおよびソフトウェアのバージョンをシスコに送信する必要があります。Dashboard の IP アドレスも記録されます。このプロセスの間に個人情報や機密情報が意図的に収集されることはありません。

ライフサイクルレポートの生成を無効にするには、以下の手順に従います。

1. [System] > [Privacy Settings] に移動します。
2. 無効にするレポートのチェックボックスをオフにします。
3. [Save] をクリックします。

Software Updates

この機能を使用するには、Cisco Business ダッシュボードが各デバイスの製品 ID とハードウェアおよびソフトウェアのバージョン情報をシスコに送信する必要があります。ローカル IP アドレスも記録される場合があります。このプロセスの間に個人情報や機密情報が意図的に収集されることはありません。

ソフトウェアの自動更新の使用を無効にするには、次の手順を実行します。

1. [System] > [Privacy Settings] に移動します。
2. デバイスファームウェアのチェックと Cisco Business ダッシュボード アプリケーションのチェックの両方のチェックボックスをオフにします。
3. [Save] をクリックします。

ログ設定の管理

[Log Settings] ページでは、各ソフトウェアモジュールによってログファイルに追加される詳細の量を制御できます。デフォルトのログ レベルは [Info] ですが、[Warn] または [Error] を選択することでログに記録されるメッセージの数を減らすことができ、また [Debug] を選択することでより多くの詳細を確認することができます。

Dashboard のログレベルを変更するには、以下の手順に従います。

1. [System] > [Log Settings] に移動します。
2. オプションボタンを使用して、各ソフトウェアモジュールの目的のログレベルを選択します。
3. [Save] をクリックします。

Dashboard のログファイルは、ローカルファイルシステムのディレクトリ `/var/log/ciscobusiness/dashboard/` で見つけることができます。[Download Log File] をクリックすると、このディレクトリのコンテンツのアーカイブをダウンロードできます。すべてのデータを収集するのに数分かかる場合があります。

syslog へのロギング

リリース2.2.1 以降、Cisco Business Dashboard アプリケーションログは、ホストの syslog サービスに送信され、そこから外部 syslog サーバに送信される場合があります。

ホスト syslog サービスへのファイルの送信を有効にするには、以下の手順に従います。

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、`/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf` ファイルを編集します。
2. `xxx.logger` 行を編集して、**file** または **syslog**、あるいはその両方を（カンマ区切りで）指定します。`redis`、`mongo`、`rabbitmq`、`nginx`、`cbd` の各モジュールを使用できます。`file` が指定されている場合、ログメッセージは `/var/log/ciscobusiness/dashboard/` ディレクトリのデフォルトログファイルに送信されます。**syslog** が指定されている場合、ログメッセージはホストの syslog サービスに送信されます。

（注） `mongo` モジュールは、複数のロギング先をサポートしません。複数の宛先がリストされている場合は、最初のエントリが優先されます。また、`cbd` モジュールは、ロガー設定の **file** キーワードの有無に関係なく、常にファイルシステムにログを記録します。

3. オプションで、`xxx.syslog.facility` 行を変更して、各モジュールに使用される syslog ファシリティを指定できます。デフォルトでは、各モジュールは、個別のローカル <*n*> ファシリティにログを記録します（<*n*> の範囲は 1 ー 5 ）。
4. **cisco-business-dashboard stop** コマンドの後に **cisco-business-dashboard start** コマンドを使用して、Cisco Business Dashboard を再起動します。

ログメッセージを **syslog** に転送するようにロギング設定を変更したら、`/etc/rsyslog.conf` ファイルを更新してログを受信し、ダッシュボードのログメッセージを目的の宛先に転送します。設定ファイルの詳細については、https://www.rsyslog.com/doc/v8-stable/configuration/index.html [英語] を参照してください。

次の手順を実行します。

1. /etc/rsyslog.conf ファイルは、ループバック インターフェイスを介してログメッセージを受信できるように更新する必要があります。次の行が追加されるようにファイルを編集して、サーバがループバック インターフェイスのみでリッスンするように制限します。

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. ディレクトリ /etc/rsyslog.d/ に新しいファイルを作成し、Cisco Business Dashboard に固有の設定ディレクティブを含めます。ファイル名は、40-cisco-business-dashboard-syslog.conf のような形式にする必要があります。

3. 手順 2 で作成したファイルを編集し、目的の宛先にログ出力を送信するためのディレクティブを含めます。たとえば、cisco-business-dashboard-logger.conf ファイルでデフォルトのファシリティを使用する場合、次の設定では、警告レベル以上のメッセージがダッシュボード アプリケーションから logger.example.com という名前の syslog サーバに送信されます。

```
local2.warning  @logger.example.com
```

4. **sudo systemctl restart rsyslog.service** コマンドを使用して rsyslog デーモンを再起動し、変更を適用します。

ローカル Probe の管理

（注） このページは AWS または Azure の Cisco Business ダッシュボード にはありません。

Cisco Business ダッシュボードプローブ は、Dashboard に対してローカルなネットワークのデバイスを管理するために、Cisco Business ダッシュボードと同じホストにインストールできます。Dashboard のシスコ仮想マシンイメージには Probe が含まれます。Dashboard に対してローカルなネットワークを管理しない場合、次の手順を使用して、同じ場所に配置されている Probe を無効にすることができます。

1. [System] > [Local Probe] に移動します。
2. トグル スイッチをクリックしてローカル Probe を無効にします。
3. [Save] をクリックします。

Dashboard から Probe ソフトウェア全体を削除するには、オペレーティングシステムにログオンし、sudo apt-get --purge autoremove cbd-probe コマンドを使用します。これに

より、Probe ソフトウェア、設定、および他のアプリケーションが必要としない依存ファイルが削除されます。

統合設定の管理

Cisco Business Dashboard は、シスコおよびその他のベンダーが提供するさまざまなアプリケーションやサービスと統合することができます。アプリケーションと統合すると、アプリケーションと実行されるネットワークアクション間でデータとイベントが交換される場合があります。

統合は、次のアプリケーションとサービスでサポートされます。

- プロフェッショナルサービス自動化（PSA）ツール
  - Connectwise Manage
- コラボレーションツール
  - Webex

各タイプの統合によって提供される機能は、同じタイプのすべての統合（PSA またはコラボレーションツール）でほぼ共通です。ただし、いくつかの違いが存在するため、以下の「可能な統合」の該当するセクションを参照して、個々のアプリケーションでサポートされている機能を確認する必要があります。各統合クラスでサポートされている機能を理解するには、次のセクションを参照してください。

プロフェッショナルサービス自動化ツールの使用

プロフェッショナルサービス自動化（PSA）ツールと統合する場合、アセット管理、イベント管理、および自動化の3つの機能領域を使用できます。これらのうち、イベント管理と自動化では、ユーザーがチケットを作成および管理して、アクティブに機能を操作する必要があります。アセット管理では、通常、以下の「可能な統合」セクションで説明されている初期設定以外のユーザー操作は必要ありません。

アセットの同期の使用

アセットの同期により、Cisco Business Dashboard のネットワークデバイスのインベントリは、デバイスに関する詳細情報を含む設定レコードとして PSA に自動的に同期されます。ダッシュボードによって管理されるデバイスが正しく把握されるように、PSA の実装によって、必要に応じて、アカウンティングおよび請求関連の情報も更新されます。更新されるフィールドの詳細については、可能な統合 （26 ページ）で使用されている PSA に対応するセクションを参照してください。

アセットの同期プロセスは、毎日午前0時に自動的に行われます。即時同期が必要な場合は、[Asset Synchronization] 画面の [Sync Assets] ボタンをクリックして開始できます。Cisco Business Dashboard とコラボレーションツールが統合されている場合は、コラボレーションツールから実行することもできます。

（注） 通常、アセットの同期プロセスには数分かかり、大規模なネットワークではさらに時間がかかることがあります。

自動化チケットを使用したネットワークアクションの自動化

自動化チケットでを使用すると、特別にフォーマットされたチケットを開いて、ネットワークデバイス上でアクションを実行できます。

チケットでは、アクションをすぐに実行するか、次の変更ウィンドウで実行するかを指定できます。また、実行前に承認手順が必要な場合があります。すべての前提条件が満たされると、Cisco Business Dashboard はチケットで指定されたアクションを実行し、操作の成功または失敗でチケットが更新されます。

自動化チケットの作成プロセスは、PSA ツールによって多少異なります。使用されている PSA の自動化チケット作成の詳細については、可能な統合 （26 ページ）の対応するセクションを参照してください。

自動化チケットが作成され、ステータスが [Start] の場合、Cisco Business Dashboard はチケットを制御し、次の手順を実行します。

1. CBD は、チケットをチェックして、必要な情報がすべて存在することを確認します。問題がある場合は、内部メモが更新され、ステータスが [Needs Attention] としてマークされます。
2. チケットの形式が正しい場合は、承認が必要かどうかを確認するためにそれがチェックされます。その場合、チケットは [Needs Approval] としてマークされ、チケットが承認されるまで、それ以上のアクションは実行されません。
3. チケットがチェックされ、アクションを実行するタイミングが確認されます。チケットが今すぐ実行するように設定されている場合、ダッシュボードはすぐにアクションを実行します。アクションが次回の変更期間で実行するように設定されている場合、新しいスケジュールプロファイルが作成され、チケットが更新されてジョブが保留中であることが示されます。
4. アクションが完了すると、ダッシュボードはチケットのメモを更新し、操作の成功または失敗を示します。アクションが正常に完了した場合、チケットはクローズされます。アクションが失敗した場合は、チケットが [Needs Attention] としてマークされます。失敗の理由が解決すると、ステータスを [Start] に変更してチケットを再スケジュールするか、アクションが不要になった場合にクローズすることができます。

自動化チケットの承認は、自動化プロセスにある程度の変更制御を挿入できるオプションです。承認を必要とする自動化チケットを指定することで、アクションが実行される前にアクションを検証し、検証がチケット履歴に記録されます。

承認が必要なチケットは、次のいずれかの方法で承認できます。

1. チケットは、PSA インターフェイスを使用して直接更新できます。

2. チケットは、Cisco Business Dashboard と統合されたコラボレーションツールを介して承認される場合があります。この場合、承認と承認者の ID を記録するメモがチケットに追加されます。

通知チケット付きネットワークイベントの管理

ネットワークイベントに応答してチケットを作成できるようにするには、Cisco Business ダッシュボードモニタリングプロファイルを更新して、[Open Helpdesk Ticket] アクションを 1 つ以上の通知モニタに追加する必要があります。モニタリングプロファイルの管理に関する詳細については、モニタリングプロファイル を参照してください。

（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 を継続的に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。

[Open Helpdesk Ticket] が有効になっているモニタリングプロファイルに一致する通知が発生すると、通知ボードで新しいチケットが開かれ、対応するデバイスの設定レコードに関連付けられます。チケットの本文は、通知に関する関連情報で更新されます。

ほとんどの通知モニタでは、通知チケットのみを開くことができます。ただし、ファームウェア通知の場合は、追加のオプションを使用できます。デバイスの新しいファームウェアバージョンが検出されると、作成されたチケットを自動化チケットとして開くこともできます。これにより、次の変更期間でファームウェアの更新がデバイスに適用されます。

モニタリングプロファイルでファームウェア通知を設定する場合は、[With Automation] と [With Approval] の 2 つの追加オプションが提供されます。[With Automation] チェックボックスをオンにすると、通知チケットの代わりに自動化チケットが作成されます。チケットは、デバイス設定に関連付けられた自動化ボードで開かれ、タイプが [Upgrade Firmware to Latest] に設定されます。

最後に、次の変更期間でアップグレードが実行されるように、サブタイプが設定されます。[With Approval] チェックボックスがオンになっている場合、サブタイプは、アップグレードがスケジュールされる前に承認が必要になるように設定されます。

コラボレーションツールの使用

Cisco Business Dashboard でのコラボレーションツールの使用は、主に 2 つの領域に分類されます。

- ネットワークイベントの通知の設定と受信。
- 限定制御インターフェイスを介したCisco Business ダッシュボードとの連携動作。

次の項では、それぞれのアクティビティについて詳しく説明します。

ネットワークイベントの通知管理

ネットワークイベントに応答したコラボレーションスペースへの通知の送信を有効にするには、Cisco Business Dashboard モニタリングプロファイルを更新して、[Send To Collaboration Space] アクションを 1 つ以上の通知モニターに追加する必要があります。モニタリングプロファイルの管理に関する詳細については、「モニタリングプロファイル」を参照してください。

（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 を継続的に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。

[Send To Collaboration Space] が有効になっているモニタリングプロファイルと一致する通知が発生すると、メッセージがコラボレーションスペースにプッシュされます。メッセージには、通知の詳細などの通知に関する関連情報、Cisco Business Dashboard でデバイスを表示するためのリンク、および関連するヘルプデスクチケットを表示するためのリンク（イベント用に作成されている場合）が含まれます。

コラボレーションスペースを介した Cisco Business Dashboard との連動動作

コラボレーションツールと統合すると、Cisco Business Dashboard は、ダッシュボードのクエリとアクションを実行するために使用できるコラボレーションボットを使用した、限定されたコマンドインターフェイスを提供します。

コマンドを呼び出す際、このインターフェイスでは、ユーザーがコマンドを受け入れるためにボットを指定する必要があります。インターフェイスは入力の柔軟性をある程度許容しますが、自然言語処理を提供するものではなく、定義済みコマンドのセットに制限されます。次の表に、使用可能なコマンドと関連アクションを示します。

表 *1*: サポートされるコラボレーションコマンド

コマンド	説明
メニュー ヘルプ ?	使用可能なすべてのコマンドのリストと説明を表示します。
Approvals	承認が必要な自動化チケットのリストを表示します。 このコマンドは、ダッシュボードがプロフェッショナルサービス自動化ツールと統合されている場合にのみ使用できます。
Approve <Ticket#>	指定された自動化チケットを実行の承認済みとしてマークします。 このコマンドは、ダッシュボードがプロフェッショナルサービス自動化ツールと統合されている場合にのみ使用できます。

コマンド	説明
Assets	アセットの同期プロセスを開始します。 このコマンドは、ダッシュボードがプロフェッショナルサービス自動化ツールと統合されている場合にのみ使用できます。
Firmware	使用可能なファームウェアアップデートがあるすべてのネットワークデバイスのリストを表示します。
Upgrade <Serial#>	次の変更ウィンドウで指定されたデバイスのファームウェア更新を実行するようにスケジュールします。 ダッシュボードが Connectwise Manage と統合されている場合、承認を必要とする自動化チケットがこのタスク用に作成されるか、またはCisco Business ダッシュボードで直接スケジュールされます。
チケット	自動化ボードと通知ボードでオープンチケットのリストを提供します。 このコマンドは、ダッシュボードがプロフェッショナルサービス自動化ツールと統合されている場合にのみ使用できます。

可能な統合

異なる統合の設定および各アプリケーションと交換される情報の詳細については、次の対応するセクションを参照してください。

Connectwise Manage

Connectwise Manage は、マネージドサービスプロバイダーが使用するために設計されたプロフェッショナルサービス自動化ツール（PSA）です。資産管理、アカウンティングおよび課金、ヘルプデスクサービスが機能の一部として含まれています。Cisco Business Dashboard と Connectwise Manage を統合することで、ネットワークデバイスの資産レコードを最新に保ち、ヘルプデスクチケットでイベントとネットワークアクションを管理できます。

サポートされる機能

Connectwise Manage と統合すると、Cisco Business ダッシュボードは資産管理、イベント管理、および自動化の 3 つの主要領域で追加機能を提供します。

資産管理の場合、Cisco Business ダッシュボードはダッシュボードで管理される各ネットワークデバイスの Connectwise Manage で設定レコードを自動的に作成し、定期的に更新します。設定レコードには、デバイスのタイプとモデル、シリアル番号、ソフトウェア情報、保証期限、ライフサイクル情報などの情報が含まれます。デバイスがダッシュボードインベントリから削除されると、設定は非アクティブとしてマークされますが、Connectwise Manage からは削除されません。

構成レコードの作成に加えて、ネットワークデバイスタイプをConnectwise Manageの特定の製品に関連付け、その製品とその顧客に関連付けられているデバイスの数量を含むCisco Businessダッシュボード更新契約を設定することもできます。

ネットワークイベントを管理する場合、選択した通知が発生したときにダッシュボードがヘルプデスクチケットを作成するように、Cisco Business ダッシュボードモニタリングプロファイルを設定できます。これらの通知チケットには、イベントの詳細が含まれ、通知を生成したデバイスの設定レコードに関連付けられます。ファームウェア通知の場合、チケットは自動化チケットとして作成して、次の変更ウィンドウでファームウェア更新をデバイスに適用することもできます。

自動化チケットは、Cisco Business ダッシュボードがネットワークアクションを実行する特殊なチケットです。自動化チケットは、ダッシュボードが監視する専用のサービスボードで作成され、次のアクションを自動化するために使用できます。

- 設定のバックアップ
- 最新のファームウェアバージョンへのアップグレード
- デバイスの再起動
- 実行コンフィギュレーションの保存
- デバイスの削除

自動化チケットは、すぐに実行するように作成することも、次の変更時間帯に作成することもできます。実行前に承認を要求するように設定することもできます。チケットは、実行中の進捗情報と完了時のアクションの結果で更新されます。

前提条件

Connectwise Manage 統合を設定する前に、次の前提条件を満たす必要があります。

- 自動化チケットを使用する場合は、Connectwise Manageアプリケーションが Cisco Business Dashboard Web サーバーへの接続を確立できる必要があります。さらに、Cisco Business Dashboard には、Connectwise Manage によって信頼されている証明書が必要です。ほとんどの場合、これは、証明書が公的 CA によって署名される必要があることを意味します。Cisco Business Dashboard の証明書の設定の詳細については、証明書の管理 （5 ページ）を参照してください。
- ダッシュボードが NAT ゲートウェイまたはファイアウォールの背後にある場合は、**[System]** > **[Platform Settings]** の [System Variables] ページに、Connectwise Manage アプリケーションがダッシュボードへの接続に使用するホスト名と Web サーバーポートが入力されていることを確認してください。
- Cisco Business ダッシュボード 用に一連の API キーを作成し、少なくとも次の表に示す権限が必要です。

表 *2 : API* キーに必要な権限

権限	追加レベル	編集レベル	削除レベル	問い合わせレベル
企業				
企業の保守	なし	なし	なし	すべて
コンフィギュレーション	すべて	すべて	すべて	すべて
ファイナンス				
契約	なし	すべて	なし	すべて
調達				
製品カタログ	なし	なし	なし	すべて
サービスデスク				
サービスチケット	すべて	すべて	すべて	すべて
システム				
テーブルの設定	すべて	すべて	すべて	すべて

- 自動化チケットに適したサービスボードを特定または作成する必要があります。このボードには、統合プロセス中に適用される多くの設定要件があります。このボードは、ネットワーク運用専用にすることをお勧めします。このボードの設定方法の詳細については、次のセクションを参照してください。
- 通知チケットに適したサービスボードを特定または作成する必要があります。このボードには特定の要件はなく、既存の汎用ボードを使用できます。通知ボードは、自動化チケットに使用されるものと同じサービスボードでもかまいません。

Connectwise Manage 統合の設定

Connectwise Manage 統合の設定には、いくつかの手順があります。

- Connectwise Manage サービスとの通信を確立します。
- Connectwise の企業を Cisco Business Dashboard 組織にマッピングします。
- アセットの同期プロセスを設定します。
- イベント通知と自動化のサービスボードを選択します。

ここでは、すべての設定を正しく行うための各プロセスの実行方法について説明します。

Connectwise Manageサービスとの通信の確立

1. [System] > [Integration Settings] の順に選択します。
2. Connectwise Manage 統合を表すタイルを特定し、トグルスイッチが [Enabled] に設定されていることを確認します。
3. [Settings] アイコンをクリックして [Connectwise Manage Settings] ページを表示し、[Connection] タブを選択します。
4. 表示されたフォームのフィールドに入力し、[Save] をクリックします。要求されたパラメータの詳細については、次の表を参照してください。

表 3 : [Connectwise Manage Connection] のパラメータ

パラメータ	説明
API Hostname	接続先の Connectwise Manage サービスのプロトコルとホスト名。デフォルトは https://na.connectwise.net です。
Company ID	Connectwise Manage の企業 ID。これは、Connectwise Manage GUI にログオンするときに使用される値と同じです。
Public key	Cisco Business Dashboard の Connectwise Manage で定義された API キーの公開キー。
Private key	Cisco Business Dashboard の Connectwise Manage で定義された API キーの秘密キー。

[Save] をクリックすると、Cisco Business ダッシュボードは接続をテストし、セットアッププロセスの後半で必要となる Connectwise Manage からの情報を読み取ります。この情報には、企業、設定タイプ、製品、契約タイプ、およびサービスボードのリストが含まれます。Connectwise Manage でこの情報のいずれかを変更した場合は、このページの [Refresh Connectwise Data] ボタンをクリックしてデータを再読み取りします。

Connectwise の企業をCisco Business ダッシュボード 組織にマッピングする

Cisco Business Dashboard と Connectwise Manage 間の接続を確立したら、Cisco Business Dashboard の組織を Connectwise Manage の企業にマッピングする必要があります。企業を組織にマッピングすると、Connectwise Manage でネットワークデバイスとイベントを正しい顧客に関連付けることができます。マッピングを完了するには、次の手順に従います。

1. [System] > [Integration Settings] の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Organization Mapping] タブを選択します。
3. [Import from Connectwise] ボタンをクリックします。これにより、会社のリストと組織のリストが比較され、企業名または企業 ID のいずれかが組織名と一致する場合にマッピングが作成されます。

4. 企業と組織間の任意のマッピングは、手動で行うことも、カンマ区切り値（CSV）ファイルを使用して行うこともできます。

マッピングの手動作成

1. マッピングテーブルの上にある [✚]（プラス）アイコンをクリックして、テーブルに新しいエントリを作成します。
2. ドロップダウンリストから、マッピングする企業名と組織名を選択します。

（注） 目的の企業名がドロップダウンメニューに表示されない場合は、[Connect] タブに戻り、[Refresh Connectwise Data] ボタンをクリックして会社のリストを更新します。

3. [Save] アイコンをクリックします。

CSV ファイルを使用したマッピングの作成

1. 組織と会社名の間の必要なマッピングを含む CSV ファイルを作成します。
2. 既存のマッピングのリストを含むテンプレート CSV ファイルのマッピングテーブルの上にある [Download] アイコンをクリックします。
3. テンプレートファイルが更新されたら、テーブルの上にある [Upload] ボタンをクリックして、ファイルで指定された新しいマッピングを作成します。

既存のマッピングの変更

1. マッピングの横にあるラジオボタンをクリックします。
2. [Edit] アイコンをクリックします。
3. 必要な変更を加えます。
4. [Save] アイコンをクリックします。

既存のマッピングの削除

1. マッピングの横にあるラジオボタンをクリックします。
2. **削除**アイコンをクリックします。

アセットの同期プロセスの設定

ネットワークデバイスを表す設定レコードを Connectwise Manage で作成することは、イベント管理および自動化機能が動作するための前提条件です。Cisco Business Dashboard は、Connectwise Manage の企業にマッピングされている組織内の各ネットワークデバイスの設定レコードを自動的に作成および更新します。アセットの同期を設定するには、次の手順に従います。

1. [System] > [Integration Settings] の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Asset Synchronization] タブを選択します。
3. [Createwise Configuration Types in Connectwise] ボタンをクリックします。

   これにより、3 つの設定タイプ（CBD 管理型ルータ、CBD 管理型スイッチ、および CBD 管理型 WAP）が作成され、ネットワークデバイスに適したフィールドと質問が表示されます。これらの設定タイプがすでに存在する場合は、フィールドと質問で更新されます。
4. [Save] アイコンをクリックします。

毎日午前 0 時に、Cisco Business ダッシュボードは企業にマッピングされた各組織のアセット同期を実行します。その組織内のネットワークデバイスごとに、そのデバイスに関する情報を含む設定レコードが作成されます。設定レコードがすでに存在する場合は、デバイス情報への変更で更新されます。Cisco Business ダッシュボードから削除されたデバイスに関連付けられている設定レコードは、**非アクティブ**としてマークされます。

同期プロセスの一環として、Cisco Business ダッシュボードは次のことも行います。

1. 各企業について、Cisco Business ダッシュボードは指定した契約タイプに一致する契約を特定します。
2. 各契約について、Cisco Business ダッシュボードは選択した製品に一致する追加を特定し、各デバイスタイプに関連付けます。
3. 追加ごとに、Cisco Business ダッシュボードは対応する製品が選択されているタイプのデバイスの数に基づいて数量を更新します。

これを実現するには、次の手順を実行します。

1. [System] > [Integration Settings] の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Asset Synchronization] タブを選択します。
3. デバイスタイプごとに、[Product] フィールドをクリックし、このタイプのデバイスに関連付ける 1 つ以上の製品を選択します。
4. [Agreement Type] 見出しで、更新する契約を特定する 1 つ以上の契約タイプを選択します。
5. [Save] アイコンをクリックします。

（注） 目的の製品または契約タイプがドロップダウンメニューに表示されない場合は、[Connect] タブに戻り、[Refresh Connectwise Data] ボタンをクリックします。

イベント通知と自動化のサービスボードを選択します。

これらの各機能に使用するサービスボードを指定して、イベント管理および自動化機能を有効にします。使用するサービスボードを指定するには、次の手順を実行します。

1. [System] > [Integration Settings] の順に選択します。
2. [Connectwise Manage] タイルの [Settings] アイコンをクリックし、[Ticket Settings] タブを選択します。
3. [Notification Board] ドロップダウンメニューから、ネットワークイベントに応じて作成されるチケットに使用する適切なサービスボードを選択します。
4. [Automation Board] ドロップダウンメニューから、自動化チケットを監視するサービスボードを選択します。

（注） 目的のサービスボードがドロップダウンメニューに表示されない場合は、[Connect] タブに戻り、[Refresh Connectwise Data] ボタンをクリックしてサービスボードのリストを更新します。

5. [Save] アイコンをクリックします。

   Cisco Business ダッシュボードは、自動化機能をサポートするために必要な適切なステータス値、タイプ、およびサブタイプを含むように、Connectwise Manage の自動化ボードの設定を更新します。

Connectwise Manage 統合に関する追加情報

Cisco Business Dashboard と Connectwise Manage のアセット同期を実行すると、Cisco Business Dashboard に認識される各管理対象デバイスは、管理対象デバイスの組織にマッピングされる企業に関連付けられた設定として作成されます。次の表は、設定項目フィールドと Cisco Business Dashboard によって提供されるデータとの間のマッピングを示しています。

表 *4 : Connectwise Manage Configuration* フィールドの使用方法

フィールド	説明
Configuration Name	デバイスのホスト名に設定します
コンフィギュレーションの詳細	
Type	設定タイプは、[Asset Synchronization] ページで設定されたデバイスタイプとマッピングに基づいて設定されます。
Status	デバイスがダッシュボードインベントリから削除された場合は [Inactive] に設定され、そうでない場合は [Active] に設定されます。
Model	デバイスのモデル番号。
Serial Number	デバイスのシリアル番号。

フィールド	説明
会社	
Company	[Organization Mapping] ページで定義されているデバイスの組織に対応する会社。
注記	
Vendor Notes	Cisco Business ダッシュボードによって設定が作成されたことを示すメモと、作成タイムスタンプが表示されます。
Configuration Questions	設定に関する質問には、次の情報が含まれています。 • デバイスの製品 ID：このフィールドはモデル番号に似ていますが、新しいデバイスを購入するときに使用される識別子です。 • ソフトウェアバージョン：この情報には、現在のバージョンと、リリースノート付きの最新バージョンが含まれます。 • ライフサイクル情報：保証終了日と適用されるサポート終了の詳細が含まれます。
デバイスの詳細	
IP Address	デバイスの管理 IP アドレス。
MAC Address	デバイスの基本 MAC アドレス

Connectwise Manage では、自動化チケットはチケットタイプ、サブタイプ、およびステータスに基づいて管理されます。Connectwise Manage で自動化チケットを作成するには、次の特性を持つ新しいチケットを作成します。

- サービスボードは、統合の設定時に作成された自動化ボードに設定する必要があります。
- チケットは、Cisco Business ダッシュボードが管理するネットワークデバイスを表す 1 つの設定にのみ関連付ける必要があります。
- タイプは、目的のアクションに設定する必要があります。使用可能なアクションのリストについては、次の「**自動化チケットのタイプ**」の表を確認してください。
- サブタイプは、必要な実行時間と承認が必要かどうかに基づいて選択する必要があります。使用可能なオプションのリストについては、次の「**自動化チケットのサブタイプ**」の表を確認してください。
- 自動化プロセスを開始するには、ステータスを[Start]に設定する必要があります。自動化を開始する前に追加の作業が必要な場合は、作業が完了するまでステータスを [Needs Attention] に設定できます。可能なすべてのステータス値の完全なリストについては、次の「**自動化チケットのステータス**」の表を確認してください。

承認が必要なチケットを使用する場合、Connectwise Manage または Cisco Business Dashboard のどちらも、承認者がチケットの作成者とは別の人物でなければならないという要件を適用できません。承認者は、指定されたスタッフのリストに制限することはできません。チケットを編集できるユーザ、またはコラボレーションスペースにアクセスできるユーザは、チケットを承認できます。必要に応じて、このような制限を実装するには、運用プロセスが必要です。

表 *5:* 自動化チケットのタイプ

タイプ	説明
Backup Configuration	デバイスの現在の実行設定のコピーを取得し、Cisco Business ダッシュボードに保存します。
Delete	Cisco Business ダッシュボードインベントリからオフラインのデバイスを削除します。
Reboot	デバイスの再起動
Save Running Config	起動時に使用するために、実行設定をデバイスに保存します。
Update Firmware to Latest	デバイスのソフトウェアを、シスコが公開している最新バージョンにアップグレードします。

表 *6:* 自動化チケットのサブタイプ

サブタイプ	説明
Approval Required – Run During Change Window	このアクションは承認が必要であり、チケットが承認された後の次の変更ウィンドウで実行されるようにスケジュールする必要があります。
Approval Required – Run Now	このアクションは承認が必要であり、チケットが承認されたらすぐに実行する必要があります。
Run During Change Window	アクションは、次の変更ウィンドウで実行されるようにスケジュールする必要があります。
Run Now	アクションはすぐに実行する必要があります。

表 *7:* 自動化チケットのステータス

ステータス	説明
Start	チケットで自動化の準備ができていることをダッシュボードに示します。
Needs Attention	手動による操作が必要であることを示します。このステータスは、自動化を開始する前に必要な作業がある場合に手動で設定でき、自動化アクションが失敗した場合にダッシュボードによって設定されます。

ステータス	説明
In Process	ダッシュボードはチケットをアクティブに処理しています。
Needs Approval	続行するには承認が必要な有効な自動化チケットを示します。続行するには手動による操作が必要です。
Approved	チケットが承認され、実行の準備ができていることを示します。チケットは、Connectwise Manage ユーザインターフェイスでこのステータスを選択するか、Cisco Business ダッシュボードと統合されたコラボレーションツールの承認コマンドによって承認されます。
Scheduled with CBD	Cisco Business ダッシュボードでジョブがスケジュールされていますが、まだ実行されていません。チケットはジョブが実行されると更新されます。
Complete (closed)	要求されたアクションは正常に完了しました。

Webex

Webex は、メッセージング、通話、および会議を含むコラボレーションツールおよびサービスのスイートです。Cisco Business ダッシュボード と Webex との統合により、重要なネットワークイベントを常に通知し、アクションを実行できます。デスクトップまたはモバイルデバイスで Webex アプリケーションを使用できます。

サポートされる機能

Cisco Business Dashboard を Webex と統合すると、コラボレーションスペースに通知を転送して、ユーザにネットワークイベントを通知できます。モニタリングプロファイルを更新して通知をカスタマイズし、転送するプロファイルを選択できます。

さらに、ユーザが Webex インターフェイスから特定のアクションを実行できる、制限された制御インターフェイスが提供されます。サポートされるアクションは次のとおりです。

- Cisco Business ダッシュボードによって作成されたオープンヘルプデスクチケットのリストを表示します。
- 承認が必要な自動化チケットのリストを表示します。
- 自動化チケットを承認します。
- 使用可能なファームウェアアップデートがあるネットワークデバイスのリストを表示します。
- ネットワークデバイスのアップグレードを開始します。

前提条件

Webex 統合を設定する前に、Webex ボットを作成し、コラボレーションスペースに招待する必要があります。ボットを設定するには、次の手順を実行します。

1. https://developer.webex.com/my-apps/new/bot に移動して Webex アカウントにログインします。
2. ボットを作成するためのフォームに入力します。ボットの名前、ユーザ名、説明を入力する必要があります。ボットのカスタムアイコンを提供するオプションもあります。

（注） Webex ではボット名に空白文字を含めることができますが、Cisco Business ダッシュボードではボット名を空白を含まない単一の単語にする必要があります。

3. [Add Bot] をクリックしてボットを作成します。 Webex 統合を設定するときに必要になるため、表示されるボットトークンをメモします。

メモ ボットトークンは一度だけ表示されるため、後で参照できるように安全な場所に記録することが重要です。

ボットが作成されたら、コラボレーションスペースに招待する必要があります。Cisco Business ダッシュボードとの統合用に専用のスペースを作成しますが、既存のスペースを使用することもできます。ただし、スペースのメンバーはすべてのイベントを表示でき、サポートされているすべてのコマンドを実行できるため、ネットワークを管理する権限を持つユーザのみがスペースを使用できるようにする必要があります。

スペースの作成とユーザの招待の詳細については、Webex ドキュメントまたは Webex アプリのオンラインヘルプを参照してください。

（注） ボットは、Cisco Business ダッシュボードと統合されている場合にのみ、単一のコラボレーションスペースに招待されます。複数のスペースに招待された場合、ボットの動作は予測できません。

ボットの作成に加えて、Webex インフラストラクチャが Cisco Business Dashboard Web サーバーへの接続を確立できることを確認する必要があります。ダッシュボードが NAT ゲートウェイまたはファイアウォールの背後にある場合は、**[System]** > **[Platform Settings]** の下の [System Variables] ページに、Webex インフラストラクチャがダッシュボードへの接続に使用するホスト名と Web サーバーポートが入力されていることを確認してください。

Webex の統合の設定

Webex の統合を設定するには、次の手順を実行します。

1. [System] > [Integration Settings] の順に選択します。
2. Webex 統合のタイルを特定し、トグルスイッチが [Enabled] に設定されていることを確認します。
3. [Settings] アイコンをクリックして、[Webex Settings] ページを表示します。
4. ボットの作成時に受け取ったボットトークンを所定のフィールドにコピーし、[Save] アイコンをクリックします。
5. ステータスフィールドに正しいボット名とコラボレーションスペースが表示されていることを確認します。

（注） ボットは、Cisco Business Dashboard の 1 つのインスタンスでのみ使用し、他のアプリケーションでは使用しないでください。複数のアプリケーションがボットに関連付けられている場合、動作は予測できません。

Cisco Business ダッシュボードにボットの詳細を設定したら、コラボレーションスペースに通知を転送するようにモニタリングプロファイルを設定できます。モニタリングプロファイルの設定の詳細については、モニタリングプロファイルを参照してください。

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。