FedRAMP セキュアの設定

この章では、セキュアな設定に関する Cisco Spaces FedRAMP の要件の概要について説明します。

ダッシュボードの管理者と権限の管理

この章では、ダッシュボード内のさまざまな権限レベルと、管理ユーザーの管理方法について説明します。管理ユーザーは、ダッシュボードにログインして、アカウント内のアプリケーション、ロケーション、デバイス、およびロールベースのアクセスを表示および管理できます。

管理者管理

新しいユーザーとして Cisco Spaces にオンボーディングする際、Cisco Spaces サポートチームがアカウント情報の設定や、初期オンボーディング要件の完了をサポートします。Cisco Spaces サポートチームは、新しいアカウントの作成、テナント ID の生成、アカウント番号の割り当て、および適切なライセンスタイプのプロビジョニングを行います。

新しいアカウントが作成されると、[**Default Admin Role**]（[**Dashboard Admin Role**]）が自動的にプロビジョニングされます。

このロールは、アカウントの作成時に設定されたユーザーの電子メールに割り当てられます。[**Default Admin Role**] は、ユーザーとロールを管理するための最上位の管理者ロールです。

ダッシュボード管理者ロール

新しいアカウントが作成されると、**デフォルトの管理者ロール（ダッシュボード管理者ロール）**が作成され、アカウント作成時に使用されるユーザーの電子メールに割り当てられます。このロールは、ユーザー/ロール管理における最上位の管理者ロールとして機能します。

デフォルトの管理ロール：機能

このロールを持つユーザは、次のこともできます。

- デフォルトの管理者ロールを持つ新しいユーザーを招待し、完全な場所または制限された場所の権限を割り当てます。
- 新しいユーザーを招待し、場所ベースの制限があるカスタムロールに割り当てます。
- カスタムユーザーロールを管理します（ユーザーロールの変更を含む）。
- 他のデフォルト管理者またはカスタムロールユーザーをアカウントアクセスから削除します。
- 次のいずれかのカスタムロールを作成します。
  - デフォルト管理者ロールアクセスのミラーリング、または
  - アプリケーション固有のアクセス権やロケーションベースの制限を付与します。
- ロールの割り当てを管理します。これには、ロールのマッピングの作成、アプリケーション/ロケーションアクセスの変更、カスタムロールの削除が含まれます。
- アカウントライセンスの権利を持つすべてのロケーション、デバイス、およびCisco Spacesアプリケーションにアクセスできます。

（注） 管理者管理セクションを介して招待されたユーザーは、アクセスが特定のアプリケーションまたは場所に制限されているかどうかにかかわらず、ユーザーとロールを管理するための Cisco Spacesアカウントで完全な管理者と見なされます。さらに、アクセスが制限されている管理者は、制限のないフル管理者を招待する機能を保持します。

デフォルト管理ロール：制限事項

このロールを持つユーザーは **次のことをできません**。

- デフォルトの管理者ロールの定義を削除または編集します。
- アカウントから自分自身を削除します。
- アカウントのライセンスまたはサブスクリプションを変更する。

アプリケーションロール

アプリケーション ロールは、表示専用アクセスから完全な設定およびデータ管理まで、ユーザーがCisco Spacesアプリケーション内で実行できることを定義します。**Read-Only**アプリケーション ロールを使用すると、ユーザーは変更を加えることなくアプリケーション UI にアクセスし、設定、レコード、および詳細を表示できます。[**Read/Write**] アプリケーションロールを使用すると、ユーザーはアプリケーション UI にアクセスして、アプリケーション関連の設定やデータを追加、編集、または削除できます。また、[**User Management**] オプションを使用して、追加のユーザー（読み取り専用または読み取り/書き込み）を招待することもできます。招待者の許可されたロケーション境界に制限されます。

読み取り専用アプリケーション ロール

ロールがアプリケーションへの [**Read-Only**] アクセスを許可している場合、次のことができます。

- アプリケーション UI にアクセスします。
- 設定、レコード、および詳細を表示します。

（注） 設定/データを追加、編集、または削除することはできません。

読み取り/書き込みロール

ロールがアプリケーションへの [**Read/Write**] アクセスを許可している場合、次のことができます。

- アプリケーション UI にアクセスします。
- そのアプリケーションに関連付けられたデータ/設定を追加、編集、および削除します。
- **User Management** オプションを **読み取り専用** または **読み取り/書き込み**として使用して、他のユーザーを招待します。範囲は、招待するユーザーの許可された場所の範囲に限定されます。

カスタムロケーション制限ロール

場所に制限があるユーザーは次のことができます。

- 割り当てられた場所のみを表示、設定、および管理します。
- それらの場所に限定してデータおよび操作アクションを実行します。

場所に制限されたカスタムロールを持つユーザーは、割り当てられた範囲外の場所にアクセスできません。

管理者の管理ワークフロー

Cisco Spaces の管理ワークフローは、管理ユーザーとそのロールを管理するためのプロセスと手順です。これらのワークフロータスクの範囲には、新しい管理ユーザーの追加、カスタムロールの管理、ユーザーロールの変更、ロールの削除、ユーザーアクセスの取り消しが含まれます。

これらのワークフローは Cisco Spaces、アカウント内のユーザーとロールを管理するために必要な手順を定義することにより、管理のセキュリティ、組織性、効率を向上させることを目的としています。

このアプローチは、Cisco Spaces アカウントのアクセス制御が適切であり、ロール権限が遵守されることを確認するのに役立ちます。必要に応じて場所の制限を管理します。これらのワークフローを実行することで、管理者は、管理アクセスを持つユーザーを制御し、組織のニーズに応じてロールを管理し、管理プロセスの完全性とセキュリティを確保することができます。

新しい管理ユーザーの招待

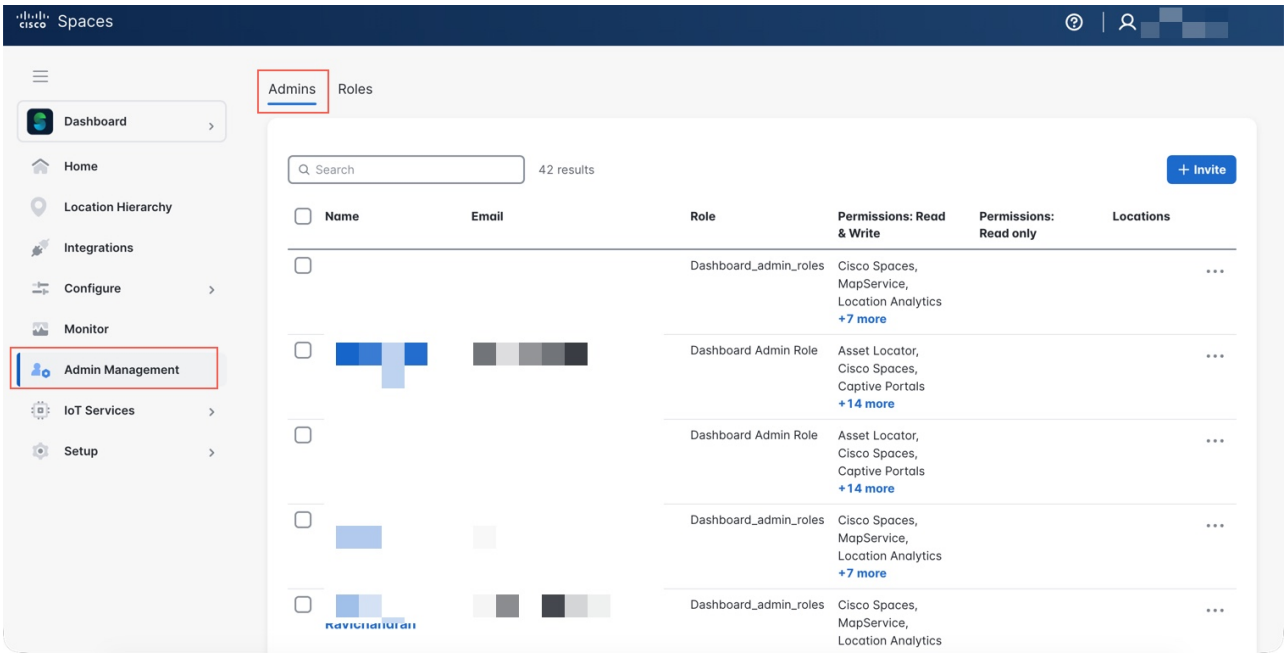
管理者が、適切な権限とアクセス範囲を持つ新しいユーザーをシステムに安全に追加できるようにします。これにより、制御されたロールベースのアクセス管理を実行できます。

このタスクでは、電子メールを指定し、ロールを割り当て、必要に応じて場所の制限を設定することにより、新しい管理者ユーザーを招待するプロセスを管理者に説明します。

新しい管理者ユーザーを Cisco Spaces に招待するには、次の手順を実行します。

手順

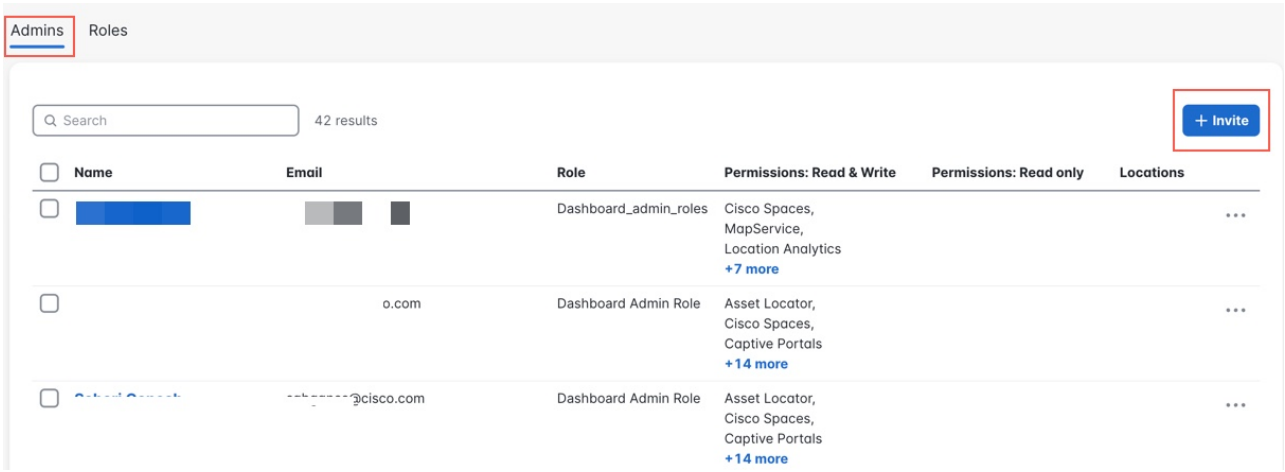
ステップ 1 左側のペインで、[**Admin Management**] をクリックします。



[**Admin Management**] ウィンドウが表示されます。

ステップ 2 [**Admins**] タブをクリックします。

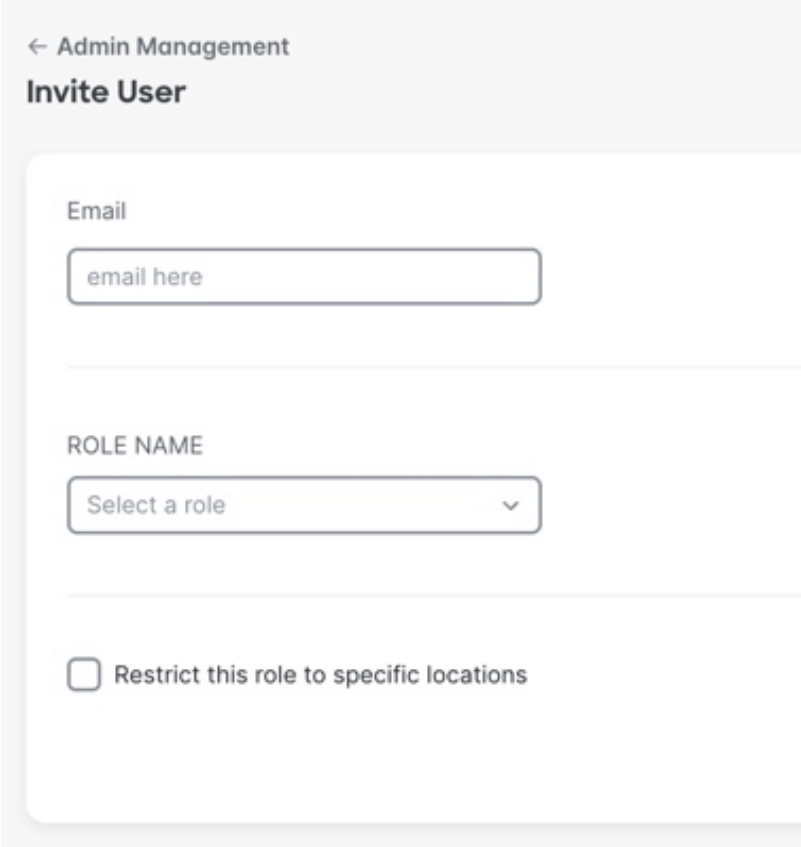
ステップ 3 新しい管理ユーザーを招待するには、[**招待**] をクリックします。



[**Invite User**] ウィンドウが表示されます。

ステップ 4 [**Email**] フィールドに、新しい管理者ユーザーの電子メールアドレスを入力します。

ステップ 5 [**Role Name**] ドロップダウンリストから、[**Default Admin Role**] またはカスタムロールとしてロールを選択します。



ステップ 6 （オプション）チェックボックスをオンにして場所の制限を有効にし、該当する場所を選択します。

ステップ 7 [**Invite**] をクリックして招待を送信します。

招待メールが新しいユーザーに送信されます。

カスタム ロールの作成

管理者が組織のニーズに合わせて調整されたロールを定義できるように、管理者権限を詳細に制御し、ロールのカスタマイズによってセキュリティを強化できるようにします。

このタスクでは、カスタム管理者ロールに名前を付け、読み取り専用、読み取り/書き込みなどの特定のアプリケーション権限を選択することで、カスタム管理者ロールを作成する方法について説明します。

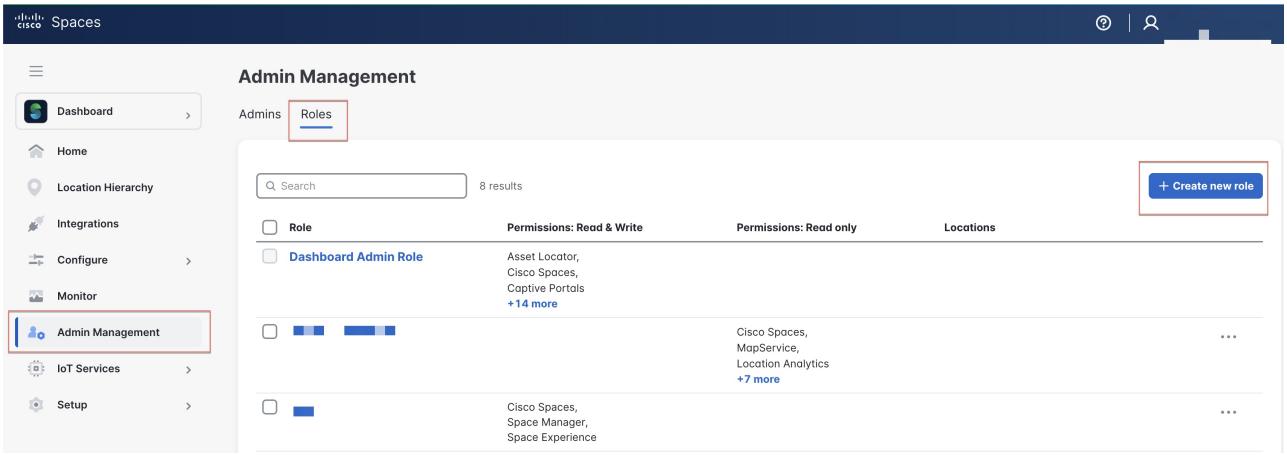
新しいカスタム管理者ロールを作成するには、次の手順に従います。

手順

ステップ 1 左側のペインで、[**Admin Management**] をクリックします。

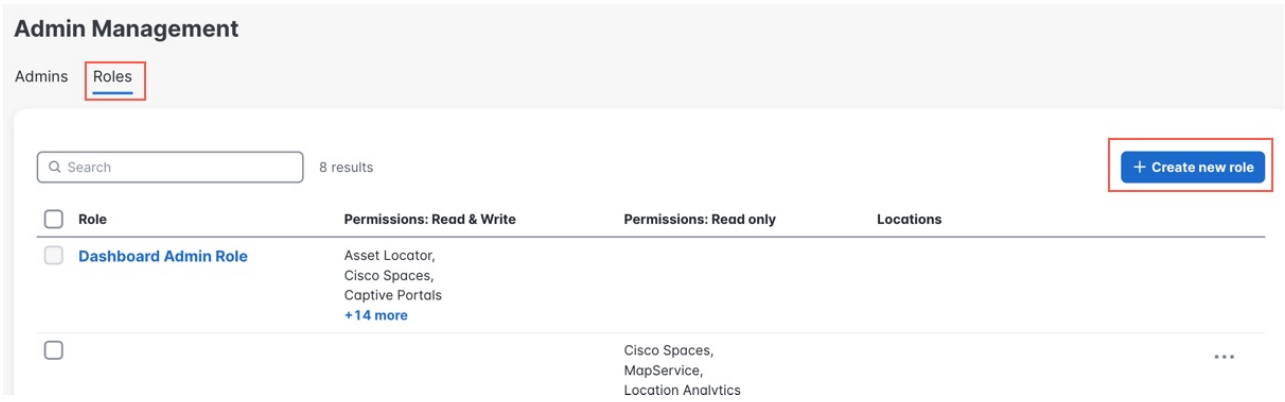
[**Admin Management**] ウィンドウが表示されます。

ステップ 2 [**Roles**] タブをクリックします。

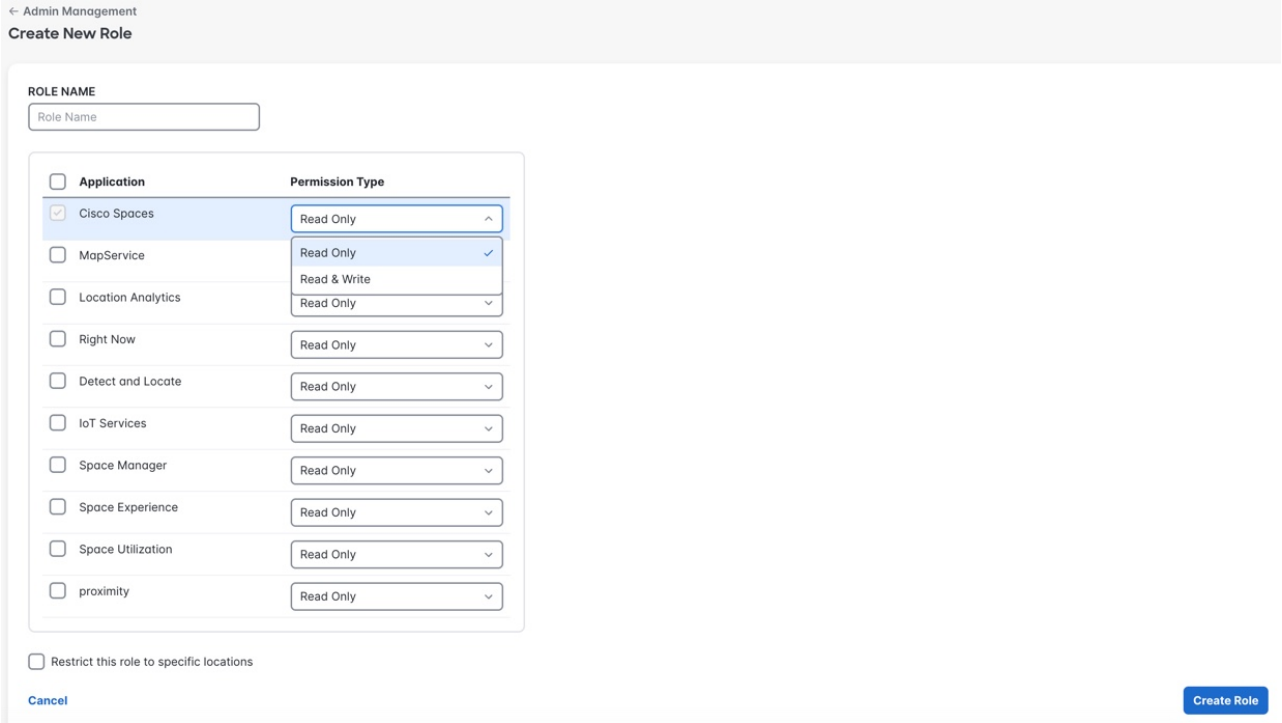


[**Roles**] タブが表示されます。

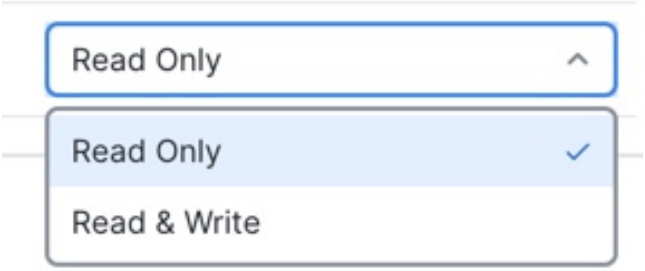
ステップ 3 新しいカスタム管理者ロールを作成するには、[**Create new role**] をクリックします。



ステップ 4 [**Role Name**] フィールドに、新しいロールの名前を入力します。



ステップ 5 [**Permission Type**] ドロップダウンリストから、権限タイプとして [**Read Only**] または [**Read & Write**] アクセスを選択します。



ステップ 6 （オプション）チェックボックスをオンにして場所の制限を有効にし、該当する場所を選択します。

ステップ 7 [**Create Role**] をクリックして、ロールを作成します。
新しいカスタムロールが正常に作成されました。

ユーザーロールの割り当ての編集

正確かつ最新のロール割り当てを維持し、管理者ユーザーがその責任に合わせた適切な権限とアクセス権を持つようにします。

このタスクでは、既存の管理者ユーザーのロールやロケーション範囲を変更する手順について詳しく説明しています。

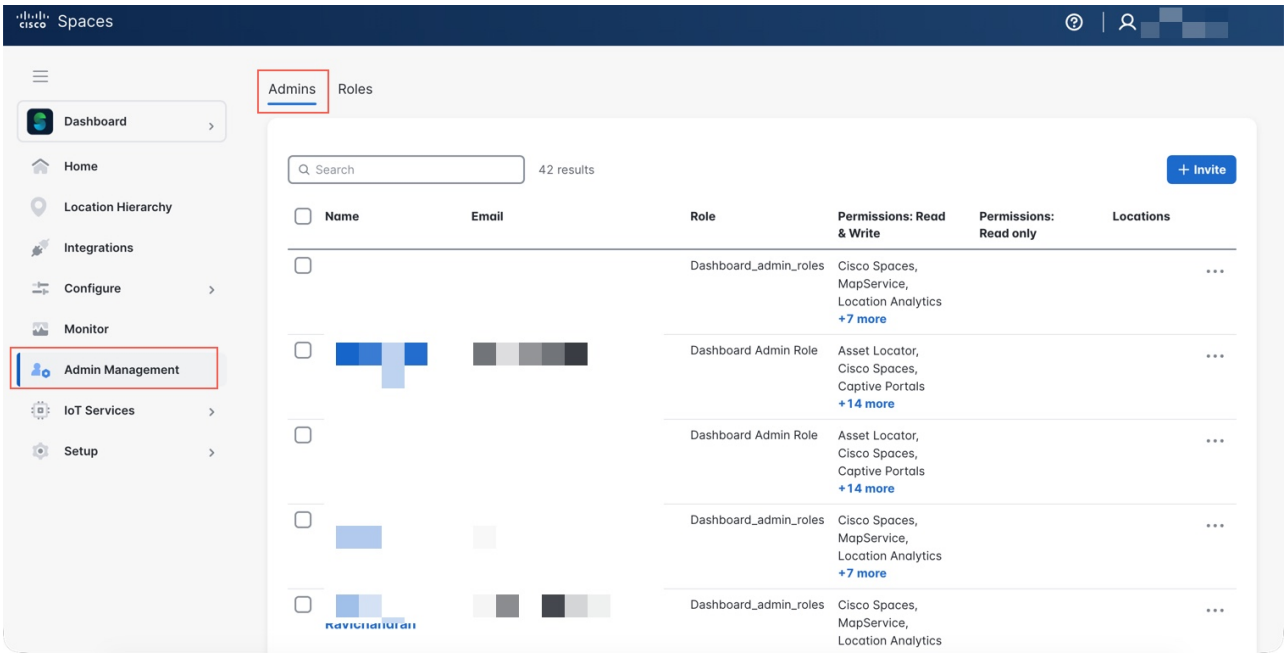
既存の管理者ユーザーのロールの割り当てを編集するには、次の手順を実行します。

手順

ステップ 1 左側のペインで、[**Admin Management**] をクリックします。

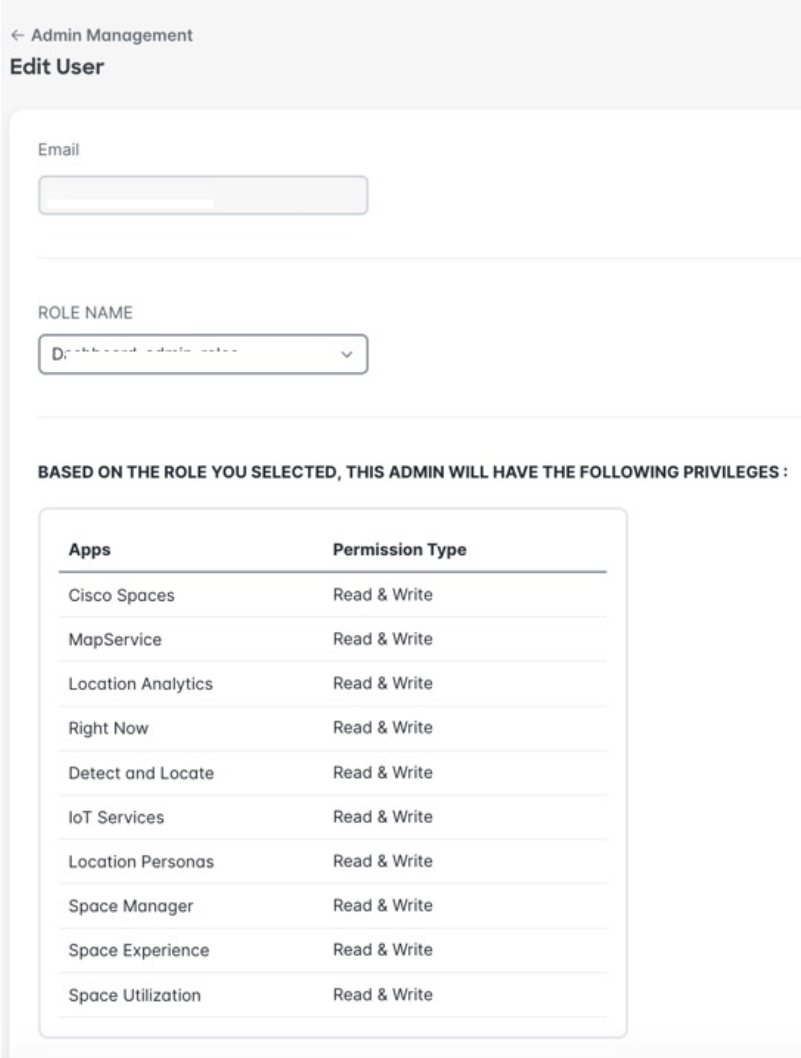
[**Admin Management**] ウィンドウが表示されます。

ステップ 2 [**Admins**] タブをクリックします。



ステップ 3 編集するユーザー名を選択して [**Edit**] をクリックします。

ステップ 4 必要に応じて、ユーザーのロールや場所の範囲を更新します。



ステップ 5 [**Update**] をクリックして変更を適用します。

カスタムロールの削除

廃止されたロールや不要なロールを削除することにより、管理ロールを管理およびクリーンアップすると同時に、適切なアクセス権を持たないユーザーが存在しないようにして、システムの完全性を維持します。

このタスクでは、カスタム管理者ロールを削除する方法と、必要に応じて影響を受けるユーザーを再割り当てすることの重要性について説明します。

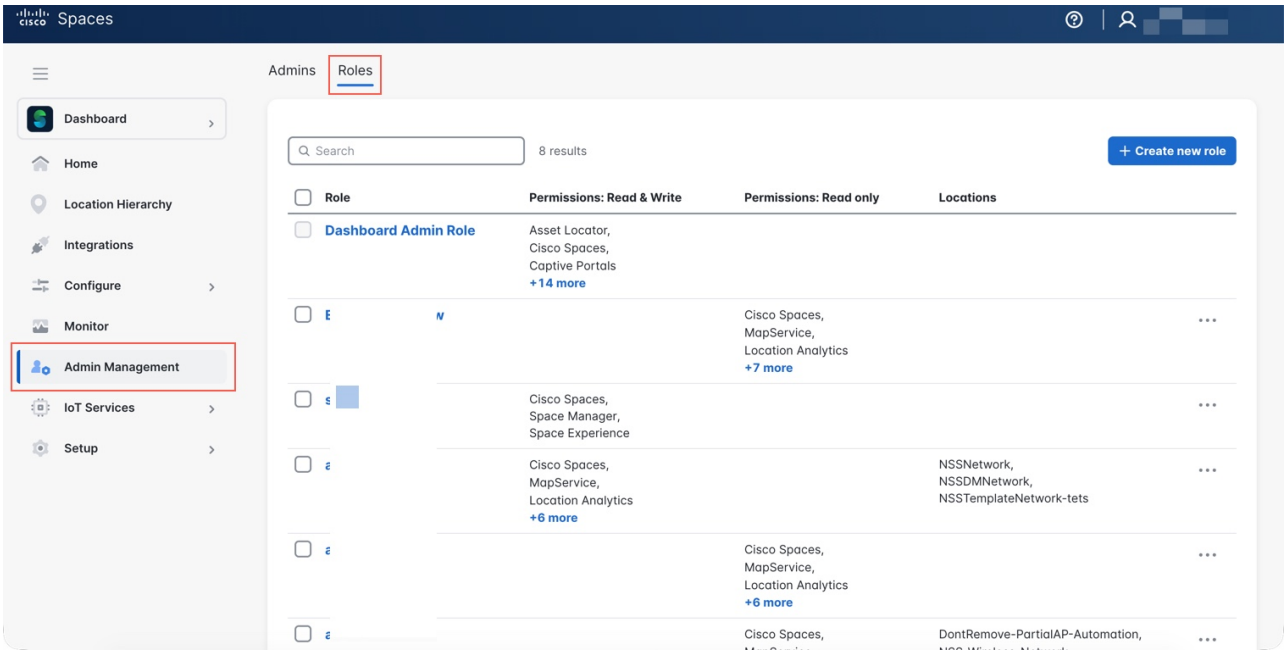
カスタム管理者ロールを削除するには、次の手順に従います。

手順

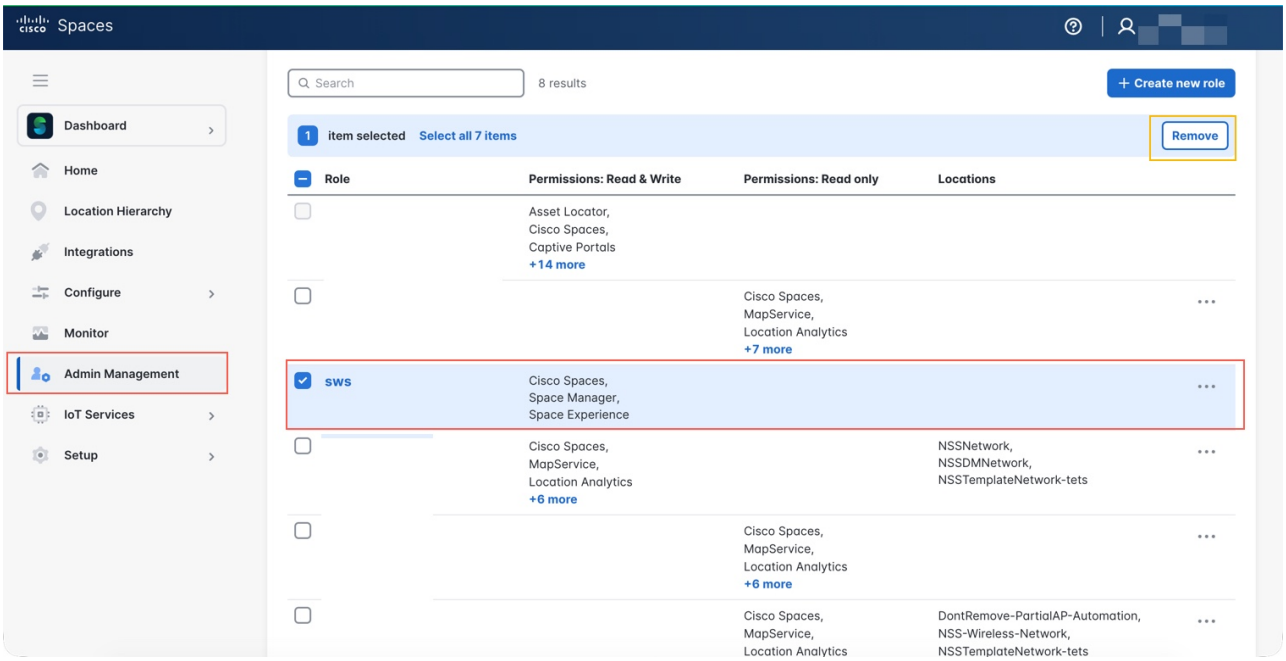
ステップ 1 左側のペインで、[**Admin Management**] をクリックします。

[**Admin Management**] ウィンドウが表示されます。

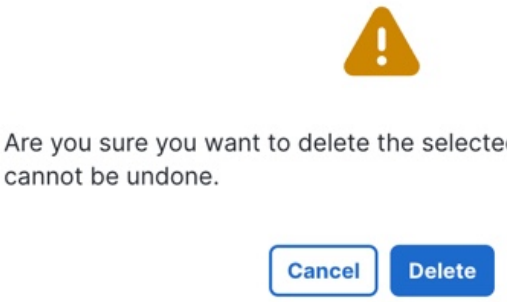
ステップ 2 [**Roles**] タブをクリックします。



ステップ 3 削除するカスタムロールを選択します。



ステップ 4 [**Remove**] をクリックして、削除を確認します。



ステップ 5 この削除の影響を受けるユーザーが必要に応じて他のロールに再割り当てされていることを確認してください。

ユーザーのアクセスを削除

管理者権限を必要としないユーザーのアクセスを安全に取り消し、不正アクセスや潜在的なセキュリティリスクからシステムを保護します。

このタスクでは、システムから管理ユーザーのアクセスを削除する手順の概要を説明します。

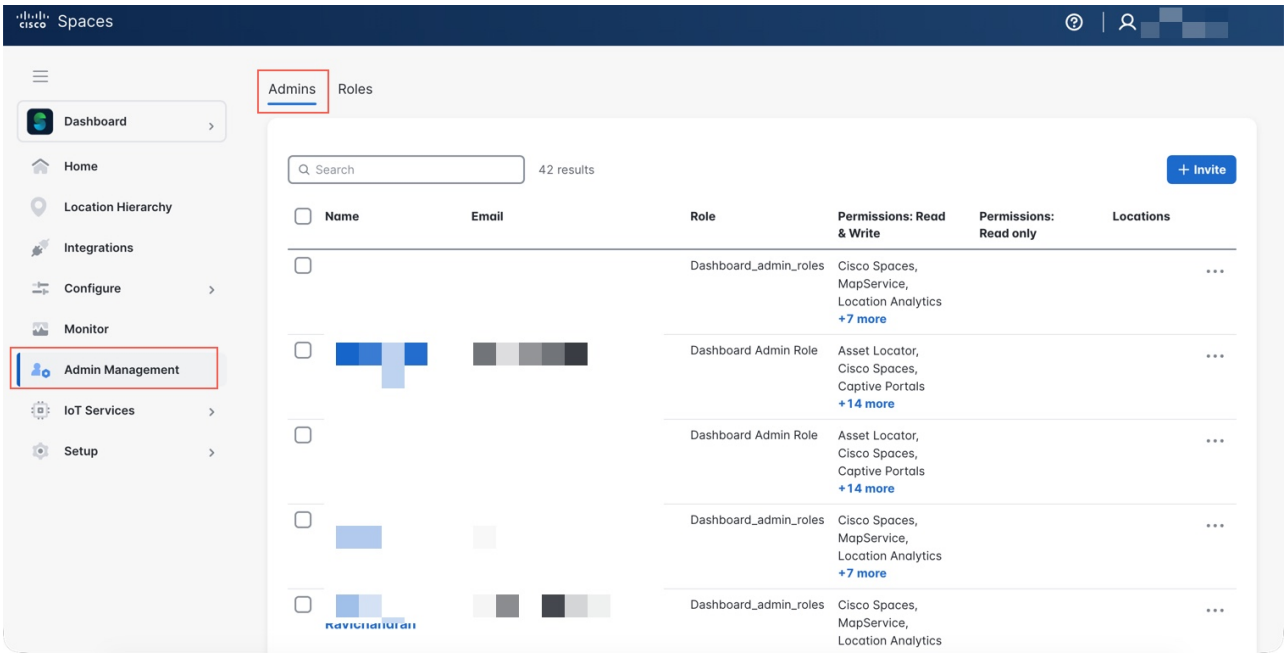
管理者ユーザーのアクセスを削除するには、次の手順を実行します。

手順

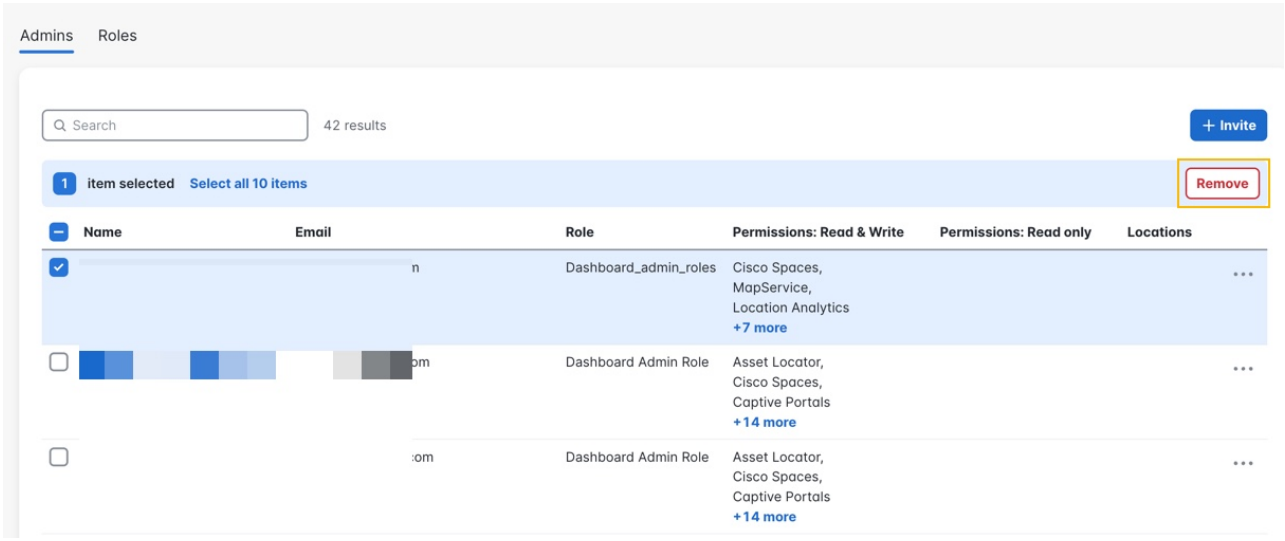
ステップ 1 左側のペインで、[**Admin Management**] をクリックします。

[**Admin Management**] ウィンドウが表示されます。

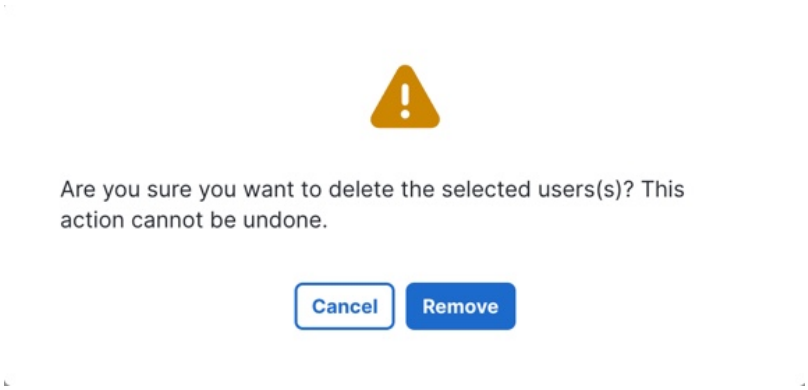
ステップ 2 [**Admins**] タブをクリックします。



ステップ 3 アクセスを削除するターゲットユーザーを選択します。



ステップ 4 [**Remove**] をクリックして、アクションを確認します。



ユーザー管理ワークフロー

ユーザー管理ワークフローは、管理者がアプリケーション内のユーザーアクセスとロールを管理できるようにする一連の構造化プロセスです。これらのワークフローには、新規ユーザーの招待、ユーザーのアクティベーションステータスの管理、招待の再送信、招待の有効期限の処理が含まれ、安全で制御されたアクセスを維持します。

ユーザー管理ワークフローの目的は、管理者がユーザーを効率的にオンボーディングするための明確で反復可能な手順を提供する一方、ロールの割り当てや場所の制限など、適切な権限とセキュリティ策を適用することです。これらのワークフローにより、招待が一定期間有効であり、必要に応じて更新できます。

主要な属性

- [**Invitation Process**]：管理者は、電子メール、ロール（読み取り/書き込みユーザーまたは読み取り専用ユーザーなど）、および場合によっては場所の制限を指定して、新しいユーザーを招待します。
- [**Invitation Resend**]：ユーザーが招待に応答しなかった場合、管理者はその招待を再送信できます。これにより、新しいトークンが生成され、招待の有効期間が再開されます。
- [**Invitation Expiry**]：招待は一定期間(5日)後に期限切れになります。その後、新しい招待が送信されない限り、トークンは無効になります。
- [**User Status Tracking**]：招待を受け入れるまで、ユーザーは「招待済み - 未応答」状態になり、保留中のユーザーアクティベーションの明確な可視性が確保されます。

ユーザー管理ワークフローは、アプリケーション内のセキュアで組織的なアクセス制御を維持するために重要です。これは、管理者が、承認されたユーザーのみが正しい権限でアクセスできること、および期限切れまたは未承認の招待によってセキュリティリスクが生じないことを確認するのに役立ちます。これらのワークフローには、ユーザー招待を組織的に管理および更新するためのメカニズムが用意されているため、業務の効率性も向上します。

- 電子メールを入力し、ロールを選択することによる、新しいユーザーの招待。

- まだ受け入れていないユーザーに招待を再送信すると、以前のトークンが無効になり、新たな有効期限を持つ新しいトークンが発行されます。
- タイムリーなユーザーアクティベーションを適用するための、5 日後に自動的に期限切れになる招待。

新しいアプリケーションユーザーの招待

適切なアクセスロールとオプションの場所の制限を含む招待メールを管理者が送信することにより、新しいユーザーをアプリケーションに追加できるようにします。

新しいユーザーの招待は、ユーザー管理の基本的な部分であり、アプリケーションへの制御されたアクセスを可能にします。このプロセスにより、ユーザーはシステムの使用を開始する前に、正しい権限と必要なロケーションベースの制限を付与できます。

Before you begin

このタスクを開始する前に、[User Management] セクションへの管理アクセス権と、招待するユーザーの電子メールアドレスを確認してください。

新しいアプリケーションユーザーを Cisco Spaces に招待するには、次の手順を実行します。

手順

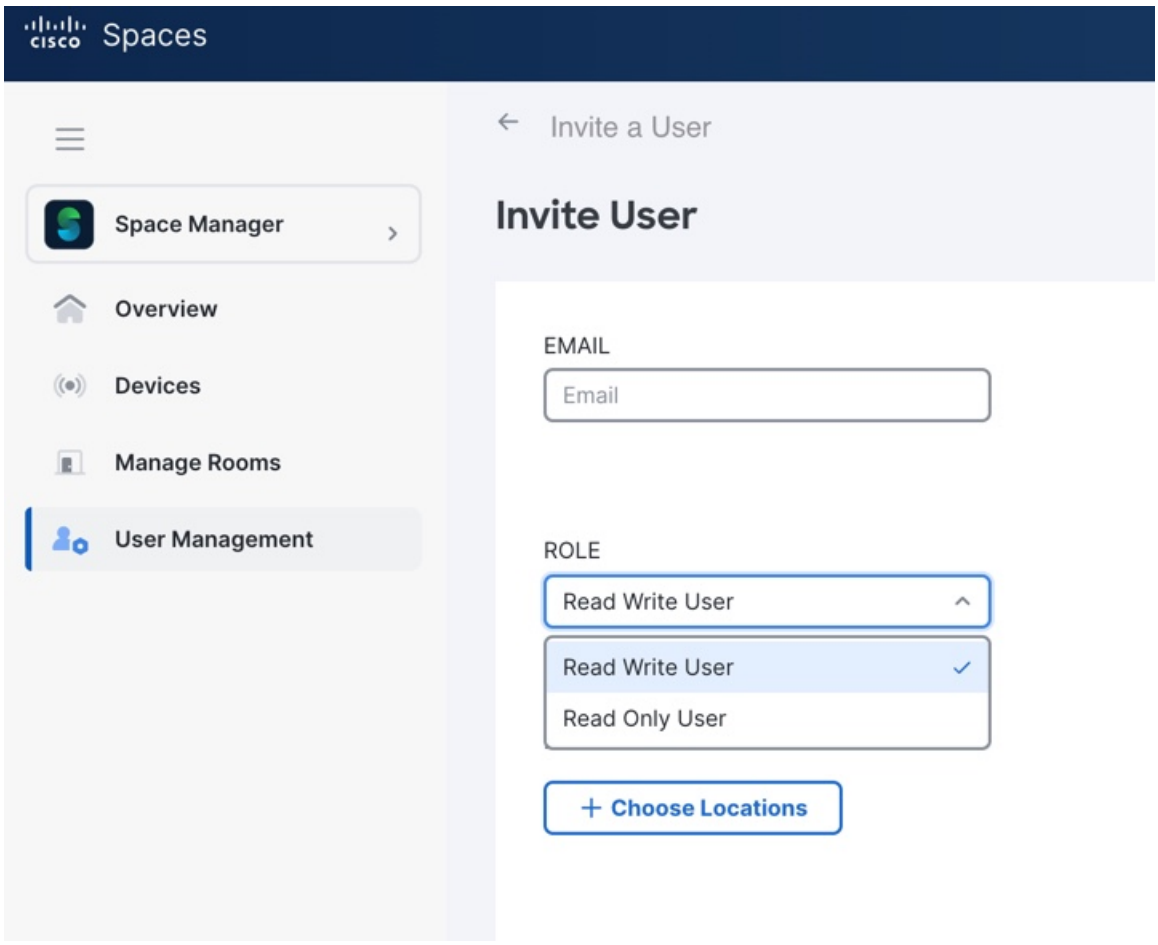
ステップ 1 Cisco Spaces：Space Manager アプリケーションの左側のペインで、[**User Management**] をクリックします。

[**User Management**] ウィンドウが表示されます。

ステップ 2 [Users] タブをクリックします。

ステップ 3 新しいアプリケーションユーザーを招待するには、[**Invite User**] をクリックします。

[**Invite User**] ウィンドウが表示されます。

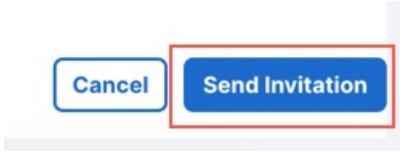


ステップ 4 [**Email**] フィールドに、新しいアプリケーションユーザーの電子メールアドレスを入力します。

ステップ 5 [**Role**] ドロップダウンリストから、ロールとして [**Read Write User**] または [**Read Only User**] を選択します。

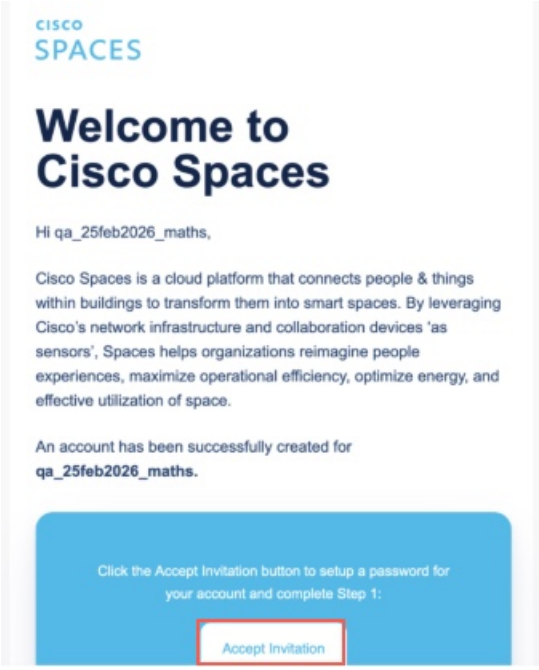
ステップ 6 （オプション）チェックボックスをオンにして場所の制限を有効にし、該当する場所を選択します。

ステップ 7 [**Send Invitation**] をクリックして、招待を送信します。



招待メールが新しいユーザーに送信されます。ユーザーが同意するまで、ユーザーステータスは [Invited - Not yet responded] に設定されます。

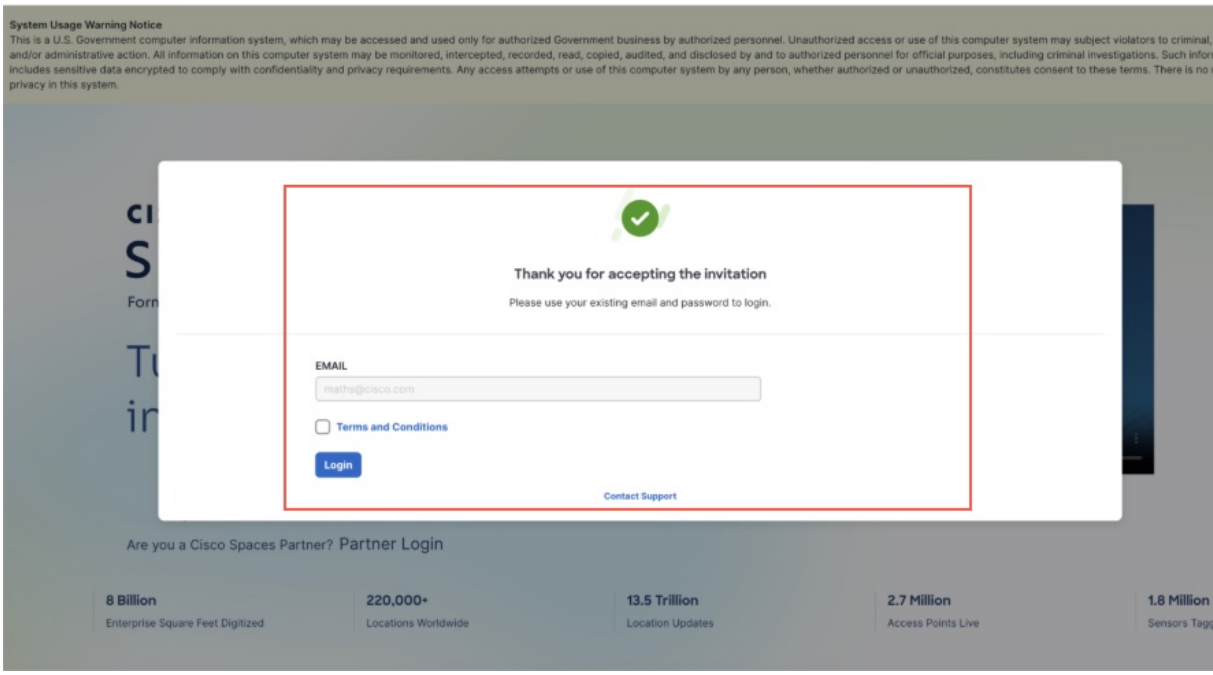
ウェルカムメールがユーザーに送信されたら、[**Accept Invitation**] をクリックしてアカウント



のパスワードを設定する必要があります。

次のタスク

電子メールとパスワードを使用してログインし、[**Select Customer**] ドロップダウンリストからアカウントを選択します。



招待状を再送信

管理者がまだ応答していないユーザーに招待を再送信できるように、有効な招待トークンがあることを確認し、招待の有効期間を延長します。

場合によっては、ユーザーが有効期間内の最初の招待に応答しない場合があります。招待を再送信すると、新しいトークンが生成され、5 日間の有効期限が再開されます。これにより、安全かつ最新のアクセス制御を維持できます。

このタスクを開始する前に、ダッシュボードへの管理アクセスが必要であり、ユーザーのステータスが [Invited - Not yet responded.] である必要があります。

招待状を再送信するには、次の手順を実行します。

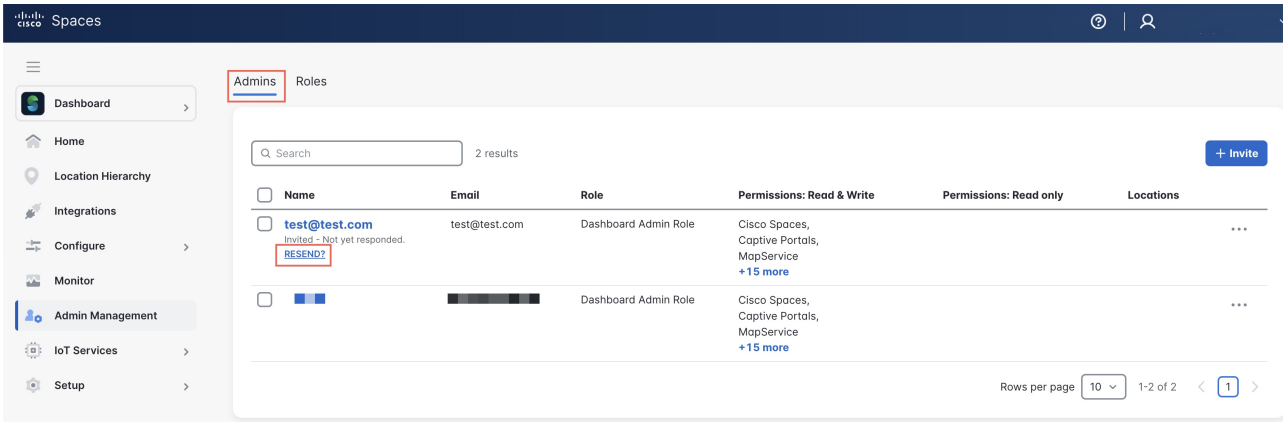
手順

ステップ 1 左側のペインで、[**Admin Management**] をクリックします。

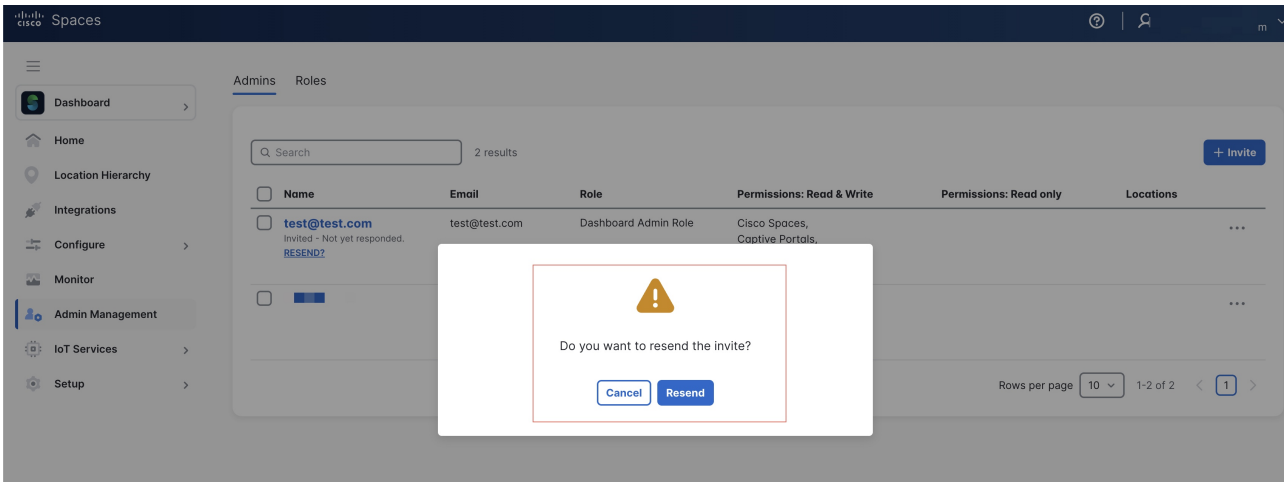
[**Admin Management**] ウィンドウが表示されます。

ステップ 2 [**Admins**] タブをクリックします。

ステップ 3 招待するユーザーを再度選択し、[**RESEND?**] をクリックします。



ステップ 4 確認ポップアップで、[**RESEND?**] をクリックします。



招待が再送信されると、新しい招待トークンが生成され、古いトークンは無効になり、使用できなくなります。招待の有効期限は、再送信した時点から5日間にリセットされ、ユーザーが招待を受け入れるまで、招待された状態のままになります。

次のタスク

招待の有効期限ルールの詳細については、招待の有効期限ルール （19 ページ） を参照してください。

招待の有効期限ルール

トークンにはセキュリティを強化するために有効期間が制限されているため、管理者がユーザーアクセスを効果的に管理するには、招待の有効期限を理解しておくことが重要です。招待を再送信すると、新しいトークンが生成されてこの期間が更新されます。これにより、ユーザーアクセスの制御が維持され、有効な招待のみがアクティブになります。目的は、ユーザー招待プロセスで使用される招待トークンの有効期限と有効性を制御するルールと動作を明確にすることです。ユーザー招待プロセスの招待トークンに関連する2つの主な属性は次のとおりです。

- [**Token Expiry**]：招待トークンの有効期間は、送信日から 5 日間です。現在時刻が期限切れ時刻未満である場合、トークンは有効であり、現在時刻が期限切れ時刻と同等以上になると期限切れになります。
- [**Token Invalidation on Resend**]：招待が再送信されると、新しい招待トークンが生成され、古いトークンは無効になり、使用できなくなります。このアクションにより、招待の有効期限が再送信時間から5日間にリセットされます。一方、ユーザーは招待を受け入れるまで、招待された状態のままです。

ルール

- 有効期限 = 招待の送信時間 + 5 日（432,000 秒）。

- トークンは、現在時刻から有効期限まで有効です。
- トークンは、現在時刻が有効期限以上になった時点で、有効期限が切れます。

[**Behavior on Resend**]

- 再送信すると、新しい発行時刻（iat）と有効期限（exp）の新しいトークンが生成されます。
- 古いトークンが無効です。
- 招待の有効期限ウィンドウが、再送信時間から 5 日間再開されます。

ガバナンスとベストプラクティス

これらのガバナンスガイドラインとベストプラクティスに従って、Cisco Spaces アカウントの安全かつ迅速な管理を実現します。

- 運用の継続のために、少なくとも2人の [**Default Admin**] ユーザーを維持してください。
- 最小権限の原則を適用し、不必要に広範な書き込みアクセス権を回避してください。
- デフォルトでは最も低い権限を使用し、不必要に広範な書き込みアクセスを回避してください。
- ビジネス境界で必要な場合は、場所の制限を使用します。
- 定期的なアクセスレビューを実行します（月次、四半期）。
- オフボーディング中にアクセスをすぐに削除します。
- ロールの作成、割り当ての変更、およびユーザーの削除の監査レコードを保持します。

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。