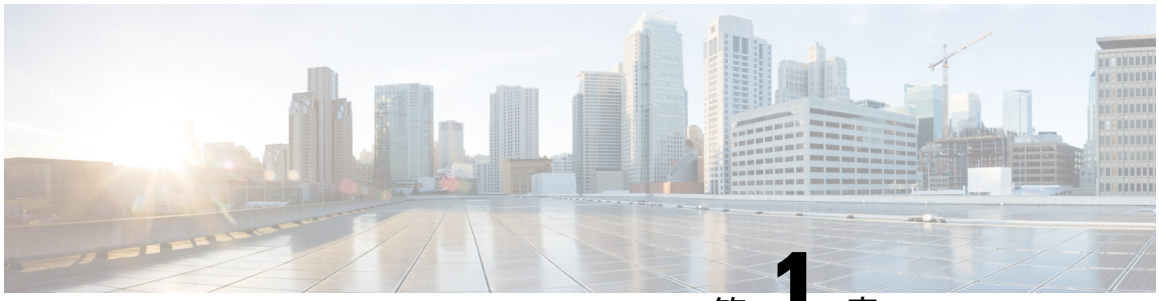
Cisco Security Provisioning and Administration ユーザーガイド

最終更新：2025 年 3 月 27 日

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

目 次



第 1 章

Security Provisioning and Administration の概要

この章では、Security Provisioning and Administration アプリケーションのナビゲーションオプションとアプリケーションにサインインする方法について説明します。

Security Provisioning and Administration の概要

Security Provisioning and Administration は、Cisco Security Cloud 全体で Cisco Secure 製品インスタンス、ユーザーアイデンティティ、およびユーザーアクセス管理を集中管理できる Web アプリケーションです。Security Provisioning and Administration の管理者は、新しい Security Cloud エンタープライズの作成、エンタープライズ内のユーザーの管理、ドメインの要求、組織の SSO アイデンティティプロバイダーの統合などのタスクを実行できます。

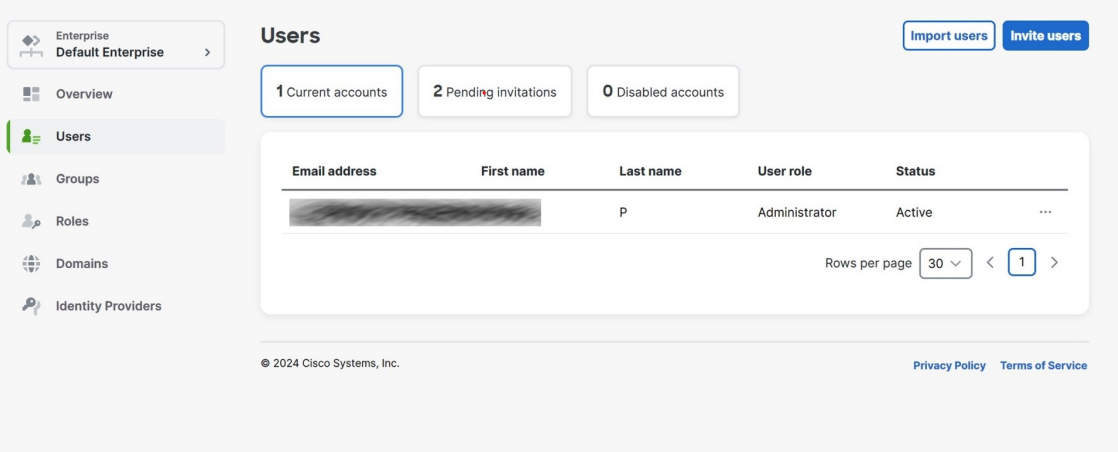
[概要（Overview）] タブ

[概要（Overview）] タブには、現在アクティブ化されているシスコ製品のインスタンスと、アクティブ化が保留中のシスコ製品のインスタンスが一覧表示されます。また、このタブからサブスクリプションを要求したり、Security Cloud に外部製品を接続したりできます。詳細については、製品およびサブスクリプションの管理 （13 ページ）を参照してください。

[ユーザー（Users）] タブ

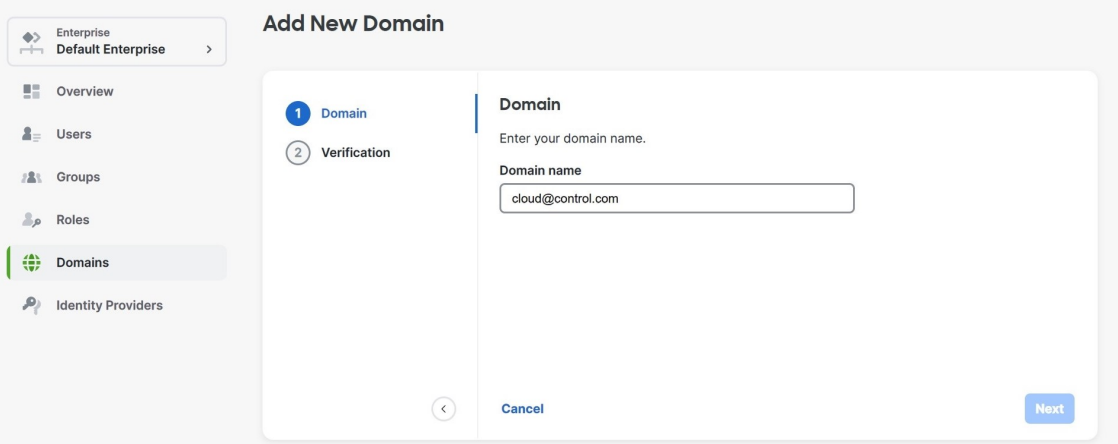
[ユーザー（Users）] タブには、エンタープライズに接続しているすべてのユーザーが一覧表示されます。エンタープライズ 管理者は、エンタープライズ にユーザーを招待して追加できます。管理者は、ユーザーパスワードと MFA 設定のリセット（要求および検証済みドメインのユーザーの場合）や、ユーザーアカウントの非アクティブ化もできます。詳細については、ロールベース アクセス コントロールの管理 （25 ページ）を参照してください。

Security Provisioning and Administration の概要



[ドメイン（Domains）] タブ

[ドメイン（Domains）] タブには、エンタープライズに対して要求および検証された電子メールドメインが一覧表示されます。ID プロバイダーを Security Cloud Sign On と統合するには、ドメインを検証する必要があります。また、管理者は、要求されたドメイン内のユーザーのパスワードまたは MFA 設定をリセットできます。詳細については、ドメインの管理 （55 ページ）を参照してください。



[ID プロバイダー（Identity Providers）] タブ

[IDプロバイダー（Identity Providers）] タブには、現在のエンタープライズについて、SAML（Secure Assertion Markup Language）を使用して Security Cloud Sign On と統合されている ID プロバイダーが一覧表示されます。これにより、エンタープライズユーザーは、ID プロバイダーの SSO 認証情報を使用して Cisco Secure 製品にアクセスできます。詳細については、ID プロバイダー統合ガイド （57 ページ）を参照してください。

Security Provisioning and Administration へのサインイン

Security Provisioning and Administration アプリケーションにサインインするには、Cisco Security Cloud Sign On アカウントが必要です。アカウントがない場合は、アカウントを作成し、Duo MFA または Google Authenticator のいずれかを使用して多要素認証を設定します。Security Cloud Sign On アカウントで Security Provisioning and Administration に初めてサインインすると、エンタープライズ内の唯一のユーザーとして、Security Cloud Sign On アカウントで新しいエンタープライズが作成されます。

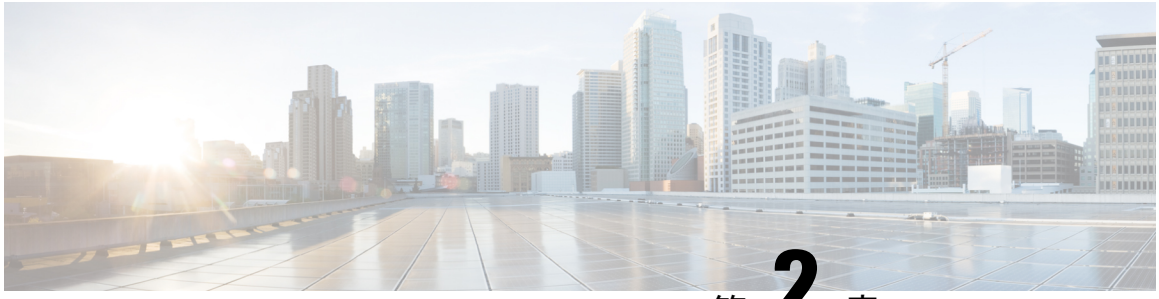
アカウントに関連付けられているエンタープライズが 1 つだけの場合は、常にログイン時のデフォルトアカウントになります。アカウントに複数のエンタープライズが関連付けられている場合は、サインイン後に選択した最後のユーザーが選択されます。

手順

ステップ 1 Security Provisioning and Administration を開きます。

ステップ 2 アカウントの作成時に設定した Security Cloud Sign On のログイン情報と MFA オプションを使用してサインインします。

Security Provisioning and Administration アカウントに初めてサインインする場合は、新しいエンタープライズが作成されます。



第 2 章

エンタープライズの管理

Security Cloud のエンタープライズは、シスコ製品、ユーザー、登録済みドメイン、ID プロバイダー、およびその他のメタデータの信頼境界です。

エンタープライズの地域の設定

エンタープライズの作成プロセス中にエンタープライズの優先地域を設定します。Security Provisioning and Administration は、この地域設定を使用して、要求されたサブスクリプションのすべての製品、およびエンタープライズ内で要求される将来の製品サブスクリプションの展開地域を調整します。製品が優先地域で利用できない場合、その製品はサポートされている地域に割り当てられ、優先地域に配置されます。優先する大陸や国と一致する展開地域が製品でサポートされていない場合、その製品はサポートされているデフォルトの地域に割り当てられます。

Security Provisioning and Administration は、製品展開地域を割り当てるプロセスを自動化し、エンタープライズ内のすべての製品に地域の連携性を確保し、相互運用性を向上させます。地域を連携させることで、エンタープライズのすべての製品が同じ地域フレームワークの下で稼働し、製品の統合が強化されます。

製品は、展開可能な地域によって制限されます。すべての製品をすべての地域に展開できるわけではありません。Security Provisioning and Administration では、ベストエフォート方式により、製品展開地域をエンタープライズの優先地域に合わせています。これは、地域の階層を調べて、可能な限り最適な地域を割り当てるアルゴリズムに従うことで実現しています。地域の割り当ての詳細については、Cisco Trust Portal で入手可能な各製品のプライバシーデータシートを参照してください。例については、Cisco Duo Privacy Data Sheet [英語] を参照してください。

例外は、スタンドアロンの Cisco XDR サブスクリプションで、展開地域は購入時の選択によって決まります。XDR サブスクリプションが要求されているか、購入地域に合わせたエンター

プライズ地域があることを確認します。すべての XDR スタンドアロン サブスクリプションは、エンタープライズ地域設定に関係なく、購入地域にデフォルトで設定されます。Cisco XDR の発注仕様と地域の選択に関するクエリについては、Cisco XDR 発注ガイド [英語] を参照してください。

地域が設定されていない既存の展開

エンタープライズに優先地域がまだ設定されていない場合、Security Provisioning and Administration にサインインすると地域の選択を求められます。地域を選択すると、エンタープライズ内にある既存の製品の展開地域は変更されません。既存のエンタープライズに対して選択した地域は、今後そのエンタープライズに追加されるすべての製品に適用できます。

既存の製品展開地域と最適な配置になるように、エンタープライズの地域を選択することを推奨します。エンタープライズの地域選択について質問がある場合は、シスコサポートにお問い合わせください。

エンタープライズの地域設定は、設定後は変更できません。エンタープライズの優先地域の調整については、Cisco Technical Assistance にお問い合わせください。

（注） 設定後に地域設定を変更すると、既存の製品の展開とデータ保持に影響を与える可能性があります。

または、異なる地域設定を使用して追加のサブスクリプション用に新しいエンタープライズを作成します。

エンタープライズの地域の設定方法については、「エンタープライズの作成」手順の「ステップ 3」を参照してください。

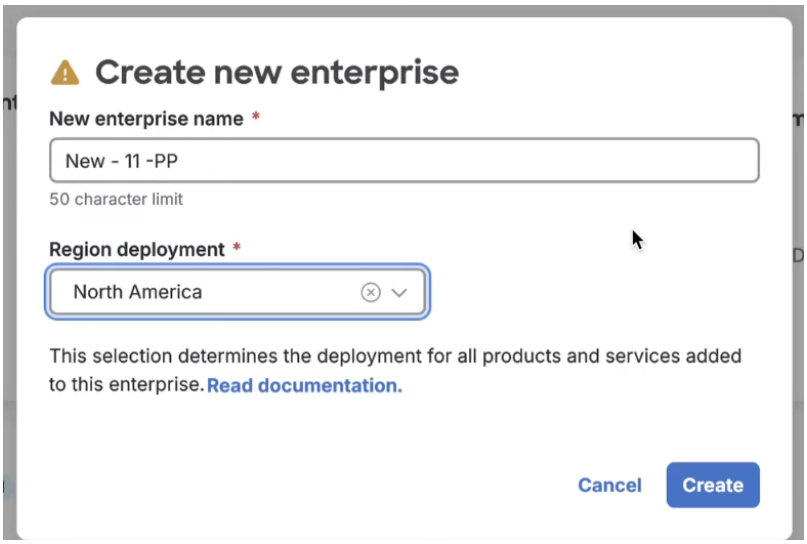
エンタープライズの作成

複数のエンタープライズを作成し、それぞれに独自のユーザー、製品、およびその他のエンタープライズデータのセットを設定できます。

手順

ステップ 1 Security Provisioning and Administration で、ブラウザの上部にある [エンタープライズ（Enterprise）] メニューにカーソルを合わせ、[新しいエンタープライズの作成（Create new enterprise）] をクリックします。

新しいエンタープライズを作成すると、現在のエンタープライズは終了します。



ステップ 2 エンタープライズの名前を入力します。

ステップ 3 エンタープライズの優先地域を設定します。

（注）

- このステップで選択する地域によって、このエンタープライズに関連付けられるすべての製品とサービスの展開可能な地域が決まります。
- エンタープライズの地域設定は、設定後は変更できません。既存のエンタープライズの地域を調整することは推奨しませんが、調整する必要がある場合は、Cisco Technical Assistance にお問い合わせください。または、異なる地域設定で追加のサブスクリプション用に新しいエンタープライズを作成できます。

  地域設定を変更すると、既存の製品展開とデータ保持に影響を与える可能性があります。

a) [地域（Region）] ドロップダウンリストから、エンタープライズの優先地域または国を選択します（[地域（Region）] ドロップダウンリストには、クラウドの導入をホストできる主な地理的地域のリストが表示されます）。

エンタープライズの優先地域に基づいて、Security Provisioning and Administration が製品の展開地域を割り当てます。製品で優先地域が直接サポートされていない場合、Security Provisioning and Administration は、階層ロジックに基づいたベストエフォート方式で、使用可能な製品展開可能な地域を優先地域に合わせます。製品に使用可能な展開地域が優先地域と一致しない場合、その製品には、使用可能な展開オプションに基づいて地域が割り当てられます。

サブスクリプションの要求プロセス中に、製品導入地域と地域設定の一致具合を確認できます。ステップ 5 ペインの [製品展開（Product deployment）] テーブルの [展開（Deployments）] フィールドには、製品の展開地域および選択した地域や国での配置を示す次のアイコンが表示されます。

- 青色のチェックマーク は、選択した地域または国が、製品でサポートされている展開地域と一致していることを示します。

- オレンジ色の三角形  は、選択した地域と類似した地域や国で製品が展開可能であることを示します。
- 紫色のアイコン  は、選択した地域に製品を展開できないことを示すため、製品は、使用可能な地域に割り当てられます。

ステップ 4 [作成（Create）] をクリックします。

新しいエンタープライズを選択した状態で Security Provisioning and Administration がリロードされます。

エンタープライズの名前の変更

作成したエンタープライズの名前を変更できます。エンタープライズの名前は 50 文字に制限されています。

手順

ステップ 1 [エンタープライズ（Enterprise）] メニューから、名前を変更するエンタープライズを選択します。

ステップ 2 Security Provisioning and Administration ページの上部にあるエンタープライズ名の横にある鉛筆アイコン をクリックします。

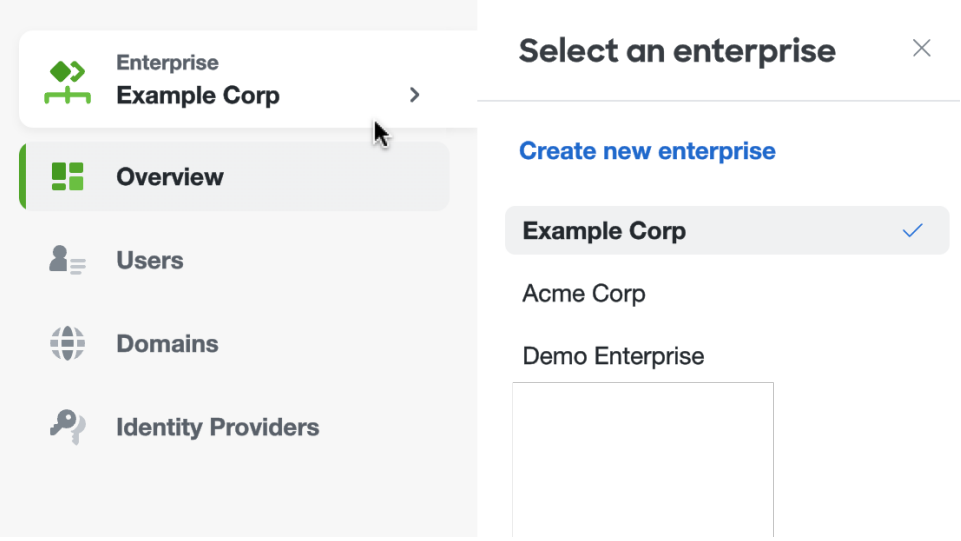
ステップ 3 [エンタープライズ名の編集（Edit Enterprise Name）] ダイアログボックスでエンタープライズの新しい名前を入力し、[保存（Save）] をクリックします。

エンタープライズの切り替え

Security Provisioning and Administration で実行するすべての操作（ドメインの作成やユーザーの招待など）は、現在選択されているエンタープライズに適用されます。Security Provisioning and Administration の上部にある [エンタープライズ（Enterprise）] メニューには、現在選択されているエンタープライズが表示されます。別のエンタープライズに切り替えるには、次の手順に従います。

手順

ステップ 1 [エンタープライズ（Enterprise）] メニューにカーソルを合わせ、スライドインペインから目的のエンタープライズを選択します。



ステップ 2 [エンタープライズの切り替え（Switch Enterprise）] ダイアログボックスで、[続行（Proceed）] をクリックします。

エンタープライズを選択した状態で Security Provisioning and Administration がリロードされます。

エンタープライズへのアクセスのサポート

サポートチームが問題をより効果的に診断およびデバッグできるように、チームにエンタープライズへの一時的なアクセス権を付与できます。このアクセスは、指定された期間が経過すると自動的に取り消され、不要になった後はいつでも無効にすることもできます。

サポートアクセスの有効化

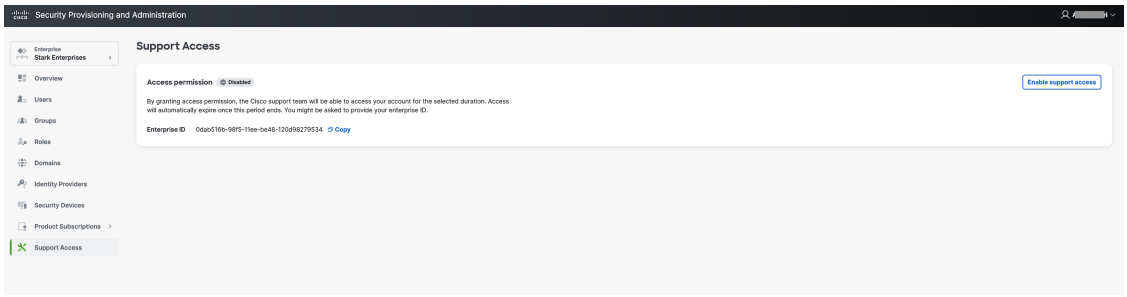
診断とデバッグを改善するために、サポートチームにエンタープライズへのアクセスを許可できます。

手順

ステップ 1 [Security Provisioning and Administration Security Cloud Control] ウィンドウで、エンタープライズ メニューにカーソルを合わせ、スライドインペインからエンタープライズを選択します。

エンタープライズを選択した状態で Security Provisioning and Administration がリロードされます。

ステップ 2 [Security Provisioning and Administration] ナビゲーションメニューで、[サポートアクセス（Support Access）] をクリックします。



ステップ 3 [サポートアクセス（Support Access）] ページで、[サポートアクセスの有効化（Enable support access）] をクリックします。

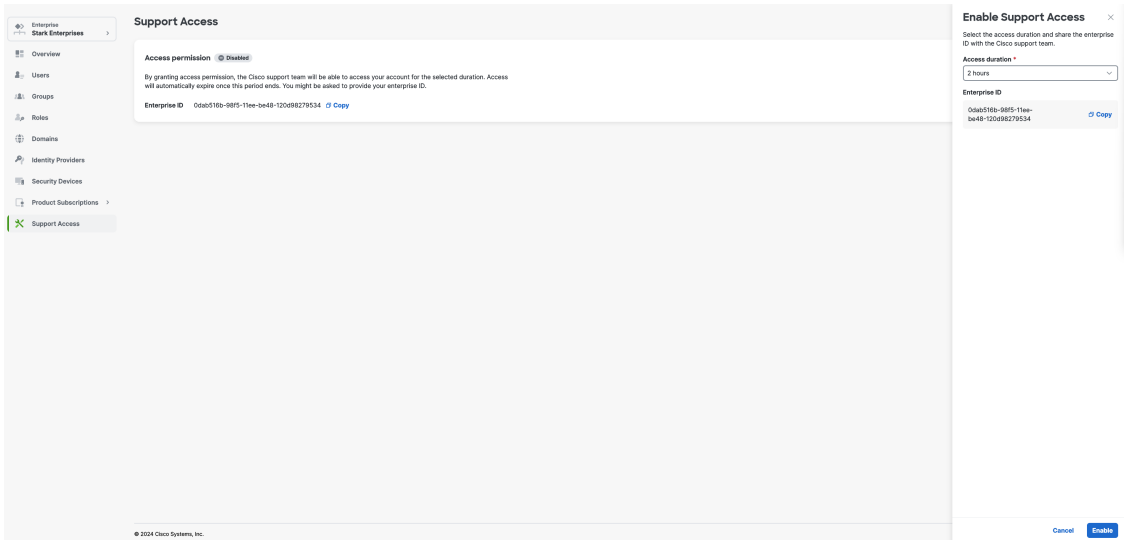
ステップ 4 [サポートアクセスの有効化（Enable Support Access）] スライドインペインで、[アクセス期間（Access duration）] ドロップダウンリストから期間を選択します。

これは、シスコサポートチームがエンタープライズアカウントにアクセスできる期間です。

ステップ 5 [エンタープライズID（Enterprise ID）] で、クリップボードアイコンをクリックして番号をコピーします。

a) エンタープライズ ID をセーフテキストツールに貼り付けます。

b) 求められたら、エンタープライズ ID をシスコサポートチームに提供します。



ステップ 6 [有効（Enable）] をクリックします。

エンタープライズへのアクセスが有効になり、サポートチームは設定した期間中エンタープライズにアクセスできます。この期間が終了すると、アクセスは自動的に取り消されます。

サポートアクセスの無効化

必要に応じて、サポートチームに提供されているアクセス権を取り消すことができます。また、アクセス期間が経過すると、アクセスは自動的に取り消されます。

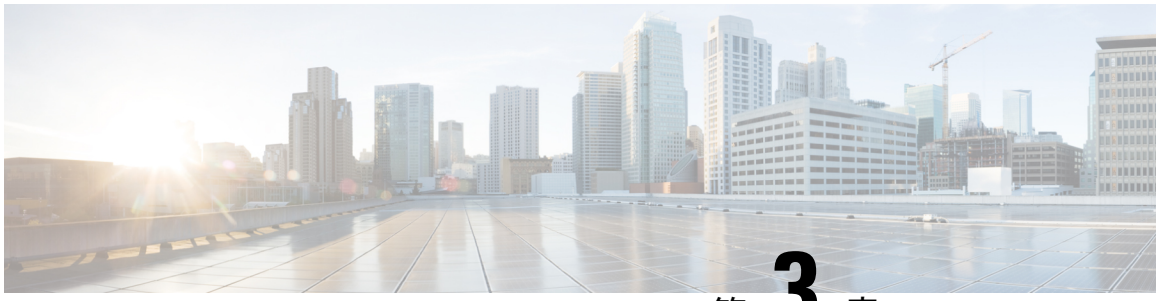
手順

ステップ 1 Security Provisioning and Administration メニューで、[サポートアクセス（Support Access）] をクリックします。

ステップ 2 [サポートアクセスの無効化（Disable Support Access）] をクリックします。

ステップ 3 [サポートアクセスの無効化（Disable Support Access）] ダイアログウィンドウで、[アクセスの無効化（Disable access）] をクリックします。

エンタープライズへの外部アクセスが無効になっています。



第 3 章

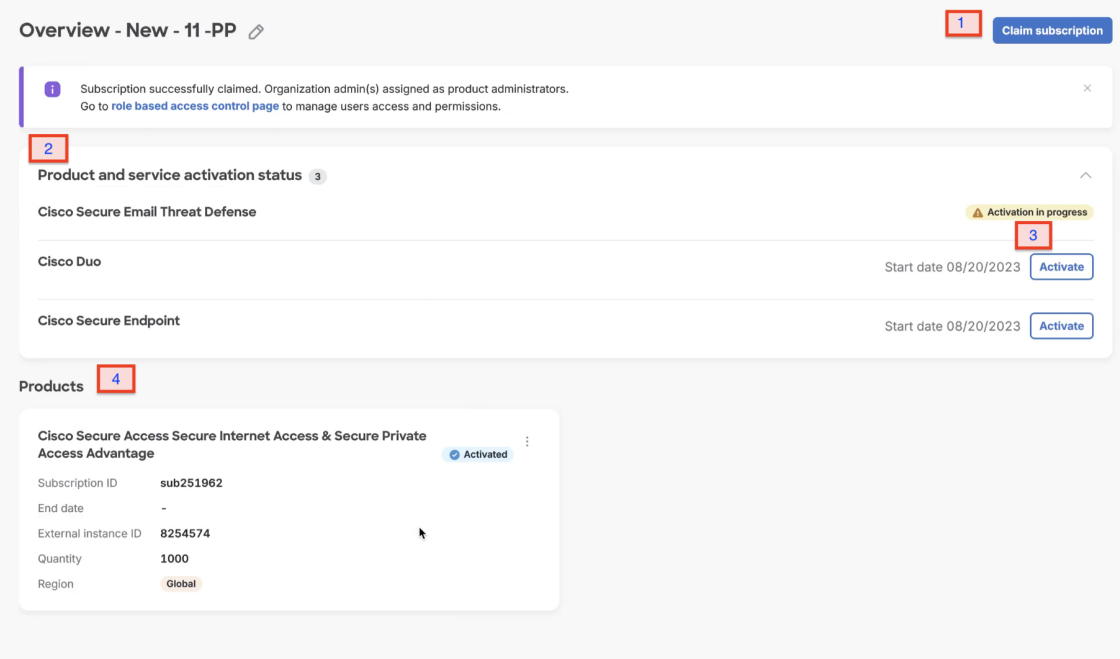
製品およびサブスクリプションの管理

この章では、要求コードの使用、製品インスタンスのアクティブ化、および外部管理インスタンスの処理を含む、Security Provisioning and Administration サブスクリプション管理プロセスについて説明します。

サブスクリプションプロセスの概要

新しいサブスクリプションをシスコから購入すると、購入プロセス中に指定した最初の連絡先にサブスクリプション要求コードを含むウェルカムメールが送信されます。Security Cloud エンタープライズ管理者は、要求コードを受信したら、[サブスクリプションの要求（Claim subscription）]（**1**）をクリックして、現在のエンタープライズのサブスクリプションを要求します。

サブスクリプションを要求すると、[製品とサービスのアクティベーション ステータス（Product and service activation status）] セクションに製品名と対応する開始日（**2**）が一覧表示されます。エンタープライズ管理者は、[アクティブ化（Activate）]（**3**）をクリックして、製品をアクティブ化します。アクティブ化された製品は、[製品（Products）] セクション（**4**）に表示されます。



アクティブ化された製品ごとに、製品サブスクリプションの詳細が個別のタイルで表示されます。

トライアル製品には Trial ラベルが付きます。Security Cloud に接続されている外部管理製品インスタンスには、Externally managed ⓘ ラベルが付きます。

（注） 製品、階層、数量の変更、共有アドオンの追加など、サブスクリプションに変更がある場合、同じサブスクリプション内ですべての変更が自動的に処理され、アクティブな製品インスタンスで更新されます。管理者は、サブスクリプションの更新に関する電子メール通知を受け取ります。

サブスクリプションの要求

最初の製品アクティベーションの連絡先として指定されたユーザーにサブスクリプション要求コードが電子メールで送信されます。管理者は、要求コードを使用してエンタープライズのサブスクリプションを要求します。サブスクリプションを要求すると、そのサブスクリプションの製品が [製品とサービスのアクティベーション ステータス（Product and service activation status）] リストに追加されます。[アクティブ化（Activate）] ボタンをクリックすると、リスト内の製品をアクティブ化できます。

エンタープライズ アグリーメント サブスクリプションの場合、ウェルカムメールと要求コードは、要求されたサブスクリプションの開始日ではなく、エンタープライズ アグリーメント ワークスペース（EAWS）内で最初の要求が行われたときに送信されます。エンタープライズ

アグリーメントのウェルカムメールと要求コードは、EAWS内で要求を行う技術担当者の連絡先に送信されます。

始める前に

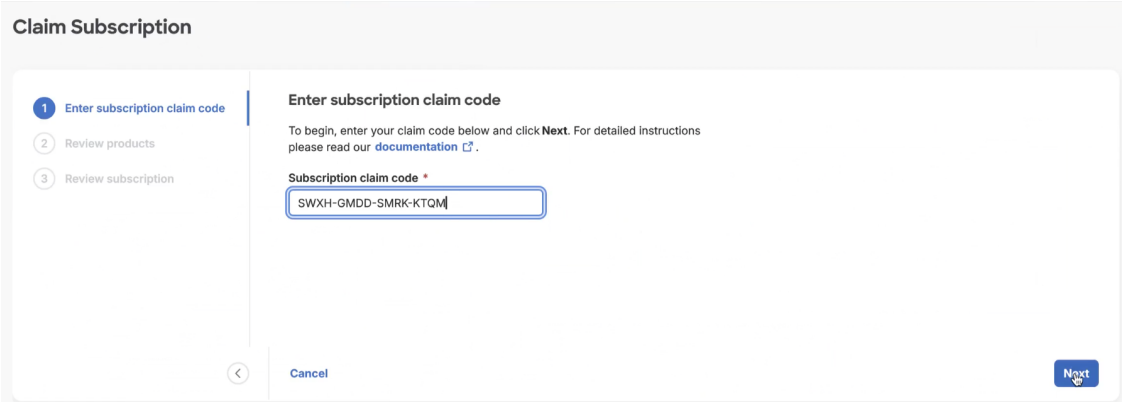
以下の手順を完了するには、サブスクリプション要求コードが必要です。

手順

ステップ1 [概要（Overview）] ページで、サブスクリプション内の製品を要求してアクティブ化するエンタープライズを選択するか、新しいエンタープライズを作成します。

ステップ2 右上隅にある [サブスクリプションの要求（Claim subscription）] をクリックします。

ステップ3 要求コードを入力し、[次へ（Next）] をクリックします。



ステップ4 サブスクリプションを製品インスタンスに関連付けます。サブスクリプションの一部である製品を確認し、サブスクリプションを関連付ける製品インスタンスを選択します。既存のインスタンスを関連付けるか、システムに新しいインスタンスを作成させます。

a) サブスクリプションに関連付ける既存の製品インスタンスの [既存のインスタンスの関連付け（Attach existing instance）] チェックボックスをオンにします。

既存のインスタンスをサブスクリプションに関連付けるプロセスを完了するには、追加の操作が必要です。製品チームまたはアクティベーション スペシャリストに連絡して、既存の製品インスタンスにライセンスを適用するプロセスを開始することもできます。

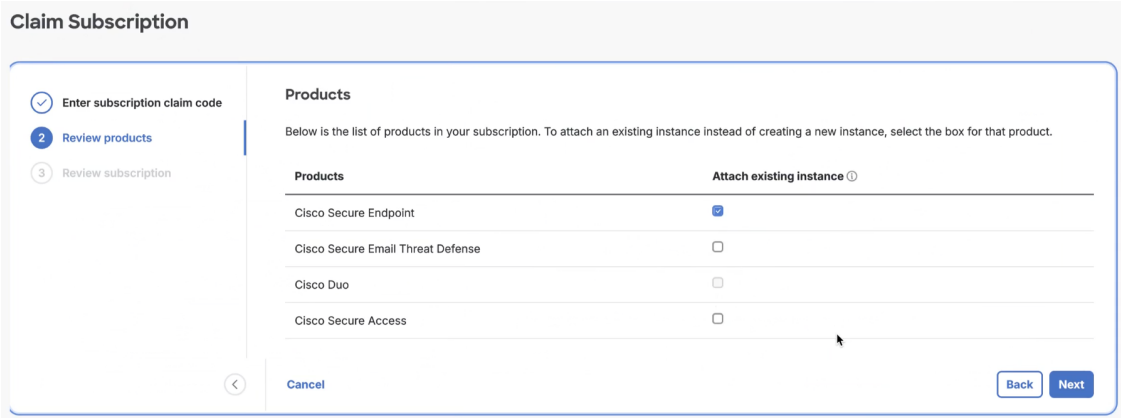
（注）
一部の製品のチェックボックスは、以下のいずれかの理由により無効になっている場合があります。

- サブスクリプションを要求後、アクティベーションを完了するために追加の手順と入力が必要な製品である。

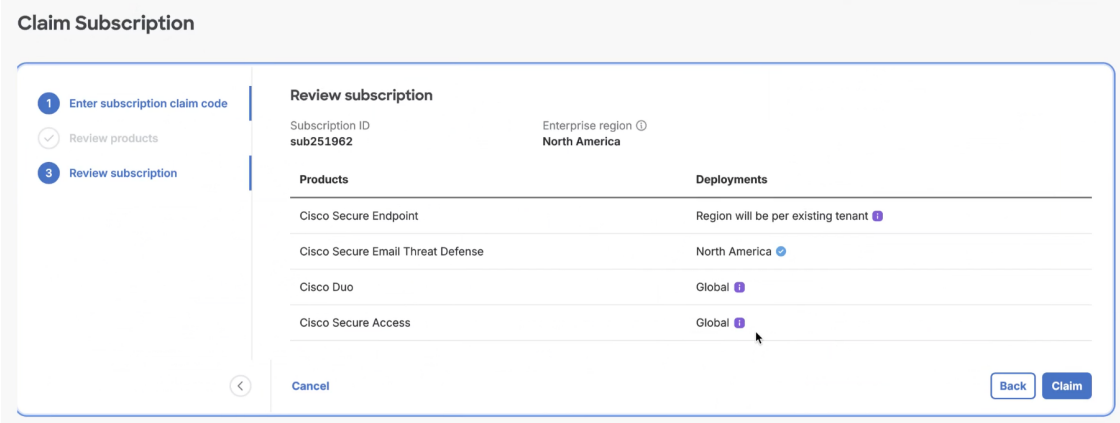
  追加の手順では、製品ごとに [必要なアクション（Action required）] オプションを使用して、必要な入力を完了します。

- 新しいインスタンスのアクティブ化のみ可能な製品である。

b) チェックボックスをオンにしていない製品の場合、製品の新しいインスタンスがサブスクリプションに関連付けられます。



ステップ 5 製品と製品に関連付けられた展開可能な地域のリストを確認し、[要求（Claim）] をクリックします。



展開地域は、既存のすべての製品インスタンスに割り当てられます。

以下のアイコンは、製品インスタンスの展開地域および選択した地域での配置を示します。

- 青色のチェックマーク は、選択した地域または国が、製品でサポートされている展開地域と一致していることを示します。
- オレンジ色の三角形 は、選択した地域と類似した地域や国で製品が展開可能であることを示します。
- 紫色のアイコン は、選択した地域に製品を展開できないことを示すため、製品は、使用可能な地域に割り当てられます。

サブスクリプションを要求する管理者には、エンタープライズ内で要求されるすべての製品の初期管理者ロールが割り当てられます。

ユーザーにロールを割り当てることで、必要に応じて管理者を追加できます。「ユーザーにロールを割り当てる （35 ページ）」を参照してください。

新しい製品インスタンスが自動的にプロビジョニングされ、[概要（Overview）] タブの [製品（Products）] リストに追加されます。既存の製品インスタンスは、アクティブ化プロセスを介してアクティブ化する必要があります。「製品インスタンスのアクティブ化 （17 ページ）」を参照してください。

（注）
製品は、要求された開始日の後にアクティブ化されます。エンタープライズアグリーメント（EA）サブスクリプションについては、製品をアクティブ化する前に、エンタープライズアグリーメントワークスペース（EAWS）で製品を要求します。EAWS 要求は、完了するまでに最大 24 時間かかります。EAWS 要求が処理されると、製品をアクティブ化できます。

次のタスク

サブスクリプションの開始日に達した製品をアクティブ化できます。

製品インスタンスのアクティブ化

サブスクリプションがサブスクリプションの要求され、その開始日に達すると、そのサブスクリプションに含まれる製品をアクティブ化できます。現在のエンタープライズでアクティブ化された既存の製品インスタンスがある場合は、新しい製品ライセンスを既存のインスタンスに適用するか、新しいインスタンスをアクティブ化するか選択できます。

（注） 製品は、要求された開始日以降にのみアクティブ化できます。

エンタープライズ アグリーメント（EA）サブスクリプションの場合は、次の手順を実行してサブスクリプションを有効化します。

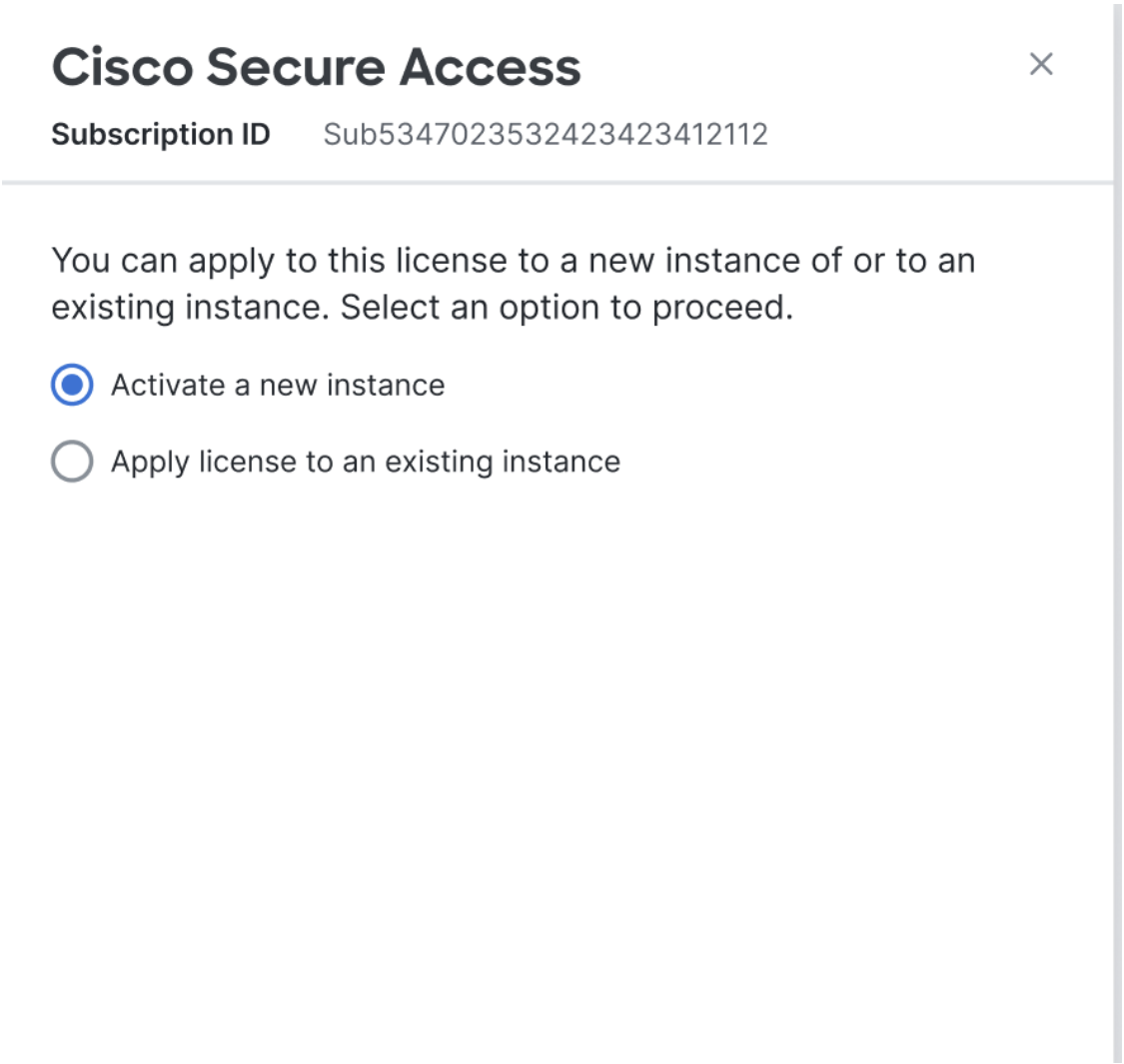
1. **EAWS でリクエストを送信**：要求された開始日以降にサブスクリプションをアクティブ化するには、まずエンタープライズアグリーメントワークスペース（EAWS）で要求を送信します。
2. **処理時間**：要求が EAWS で処理されるまでに最大 24 時間かかります。
3. **アクティベーションの有効化**：EAWS 要求が処理されると、Security Provisioning and Administration で製品アクティベーションが有効になります。次の手順を実行して、製品インスタンスをアクティブ化します。

手順

ステップ 1 Security Provisioning and Administration ページで、関連する製品サブスクリプションのサブスクリプションの要求に使用したのと同じエンタープライズを選択します。

ステップ 2 [製品とサービスのアクティベーション ステータス（Product and service activation status）] リストで、アクティブ化する製品の [アクティブ化（Activate）] をクリックします。

ステップ 3 表示されたスライドインペインで、ライセンスを既存の製品インスタンスに関連付けるか、製品の新しいインスタンスを作成するかを選択します。



既存のインスタンスをアクティブ化するには、[製品のプロビジョニング方法（How would you like to provision the product）] ドロップダウンリストから [既存のアカウントに接続（Connect an existing account）] を選択します。

製品の新しいインスタンスを作成するには、[製品のプロビジョニング方法（How would you like to provision the product）] ドロップダウンリストから [新規アカウントの作成（Create a new account）] を選択します。

ステップ 4 [アクティベーションの要求（Request activation）] をクリックします。

製品のステータスに [アクティブ化が進行中（Activation in progress）]と表示され、製品インスタンスのアクティブ化が進行中であることが示されます。この状態では、製品インスタンス ID は生成されません。アクティブ化が完了すると、製品に製品インスタンス ID が割り当てられ、製品の詳細が [製品（Products）]

セクションに表示されます。アクティブ化の完了に予想より時間がかかっている場合は、シスコサポートにお問い合わせください。

製品が [製品（Products）] テーブルに追加されます。「製品サブスクリプションの詳細の表示」を参照してください。

製品サブスクリプションの詳細の表示

[概要（Overview）]ページの [製品（Products）] セクションには、組織内で要求およびアクティブ化された関連製品を含む、各サブスクリプションの概要が表示されます。

製品インスタンスをアクティブ化すると、その製品が [製品（Products）] セクションに表示されます。

[製品（Products）] セクションの各製品カードには、アクティブ化された製品に関する次の詳細が表示されます。

- [製品名（Product Name）]：サブスクリプションで購入した製品の名前。

  名前は、購入した主要な製品（階層を含む）、およびサブスクリプションにおけるアクティブな製品の権限を識別する記述子などの関連する詳細を要約したものです。

  たとえば、Advantage 階層用に設定された Cisco XDR 製品の説明には「Cisco XDR Advantage」と表示されます。

- [サブスクリプション識別子（サブスクリプションID）（Subscription Identifier (Subscription ID)）]：サブスクリプションとその基礎となる製品に割り当てられている一意の識別子。サブスクリプションで要求される製品はすべて、このサブスクリプション ID に関連付けられます。

- [終了日（End Date）]：期間の終了日に達するようにサブスクリプションが設定されている場合の予定終了日を示します。この日付は最終的な日付ではなく、サブスクリプションが更新された場合は変更される可能性があります。サブスクリプションの最終的な終了日を取得するには、シスコテクニカルサポートにお問い合わせください。

- [外部インスタンスID（External Instance ID）]：アクティブ化される外部製品インスタンスの一意の識別子。

- [数量（Quantity）]：サブスクリプションに含まれる特定の権限付与量を示します。

- [地域（Region）]：エンタープライズの優先地域に合わせた製品インスタンスの展開地域を指定します。

外部管理対象製品インスタンスの接続

Security Provisioning and Administration の外部で管理されているシスコ製品インスタンスがある場合は、必要に応じて Security Cloud エンタープライズに接続できます。シスコは、Security Provisioning and Administration 管理者のリストに、インスタンスを Security Cloud に接続するための招待メールを送信することで、このプロセスを開始します。管理者はサインインして、外部インスタンスを Security Cloud に接続できます。Security Cloud に接続されている製品インスタンスには、製品名の横に [外部管理（Externally managed）] ラベルが付いています。

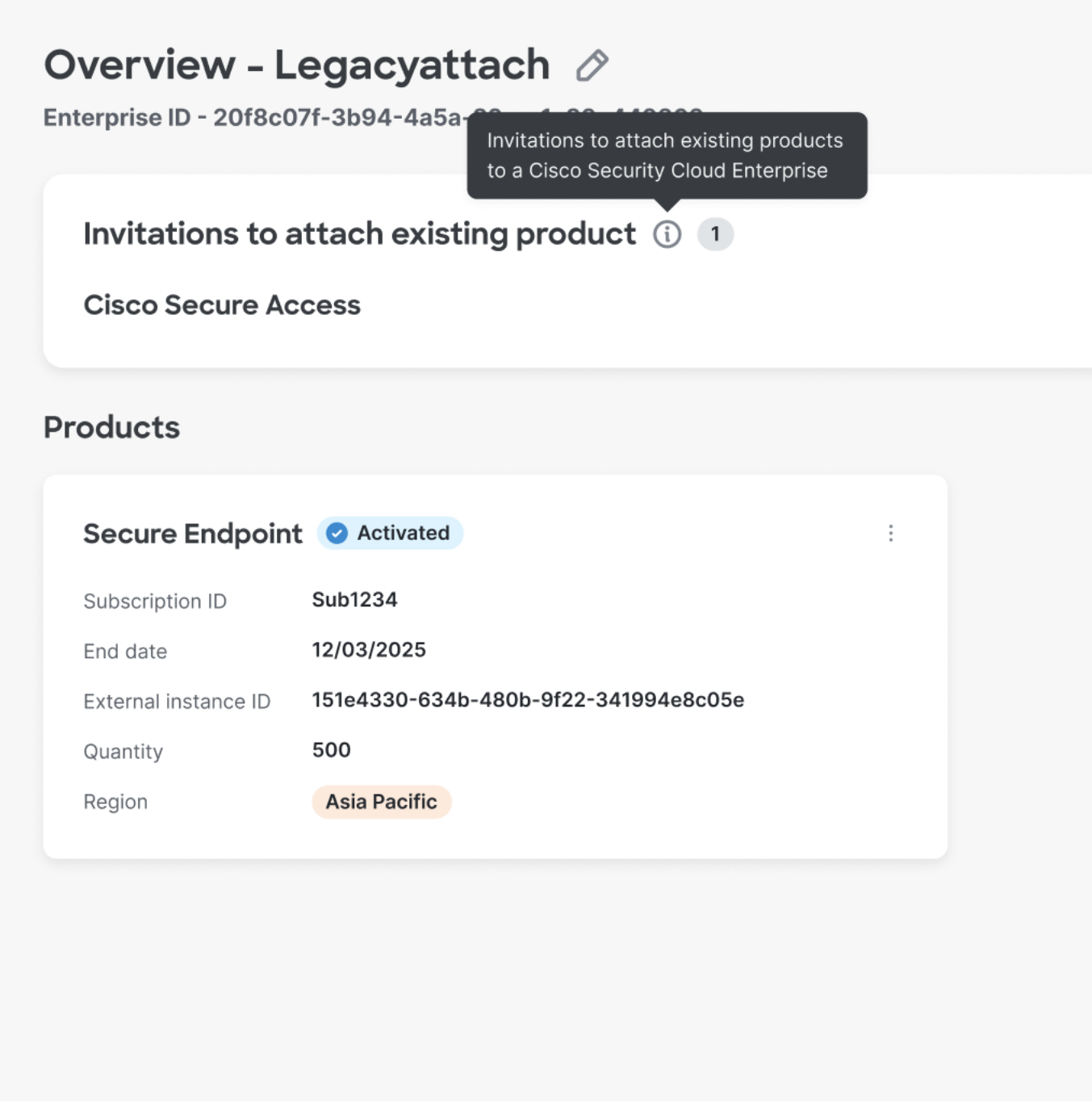
製品インスタンスの [外部管理（Externally managed）] ラベルがない場合は、インスタンスをアクティブ化せず、アクティベーション スペシャリストに相談するか、シスコサポートにお問い合わせください。

外部インスタンスをエンタープライズに接続するオプションが表示されない場合は、アクティベーション スペシャリストに相談するか、シスコサポートにお問い合わせください。

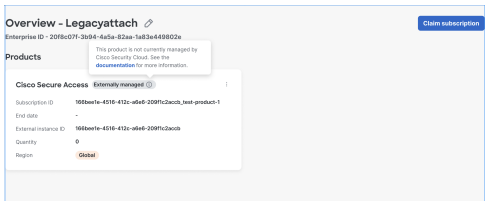
手順

ステップ 1 Security Provisioning and Administration で、外部管理製品インスタンスを接続するエンタープライズを選択します。

ステップ 2 接続する製品の横にある [製品の接続（Attach product）] をクリックします。



接続された製品は、製品のリストに外部管理ラベル付きで表示されます。



製品インスタンスの非アクティブ化

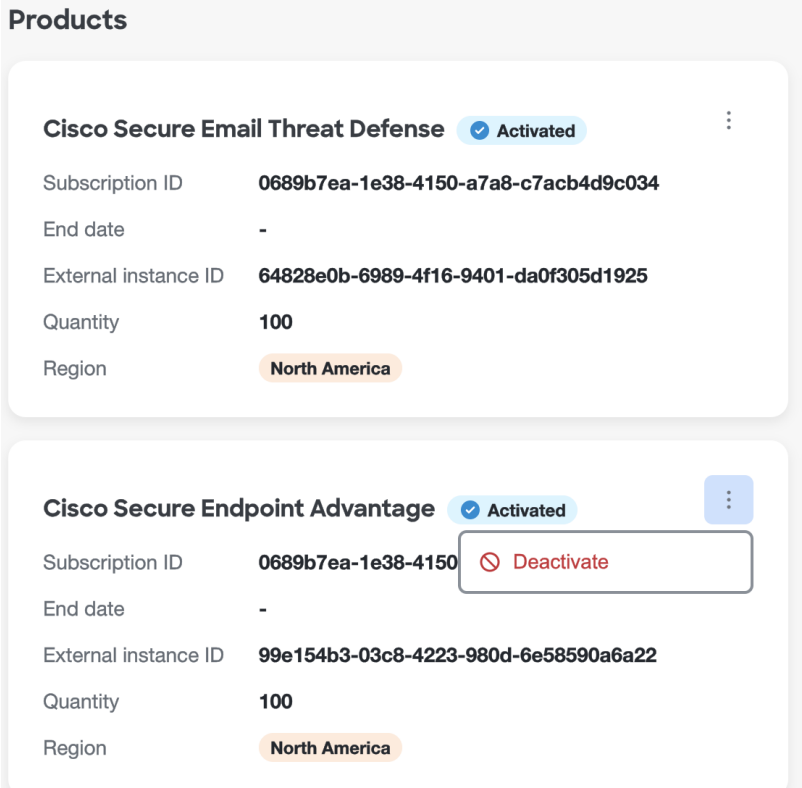
製品インスタンスを誤ってアクティブ化した場合や、既存または新しいテナントのライセンスを再利用する場合は、製品インスタンスを非アクティブ化できます。製品インスタンスを非アクティブ化すると、非アクティブ状態になります。アクティブなライセンスが再び使用可能になり、エンタープライズ管理者は製品の非アクティブ化通知を受け取ります。

（注） ライセンスのない製品インスタンスまたは外部で管理されている製品インスタンスは非アクティブ化できません。製品インスタンスをエンタープライズに誤って関連付けた場合は、シスコサポートチームにお問い合わせください。

手順

ステップ 1 Cisco Security Provisioning and Administration で、製品サブスクリプションのアクティブ化に使用したのと同じエンタープライズを選択します。

ステップ 2 [概要（Overview）]ページの[製品（Products）]テーブルで、非アクティブ化する製品の横にあるその他メニュー … をクリックし、[非アクティブ化（Deactivate）] を選択します。



ステップ 3 非アクティブ化ダイアログボックスで、[非アクティブ化（Deactivate）] をクリックします。

非アクティブ化後、製品インスタンスのすべてのサービスが一時停止され、[製品（Products）] テーブルにその製品が非アクティブと表示されます。

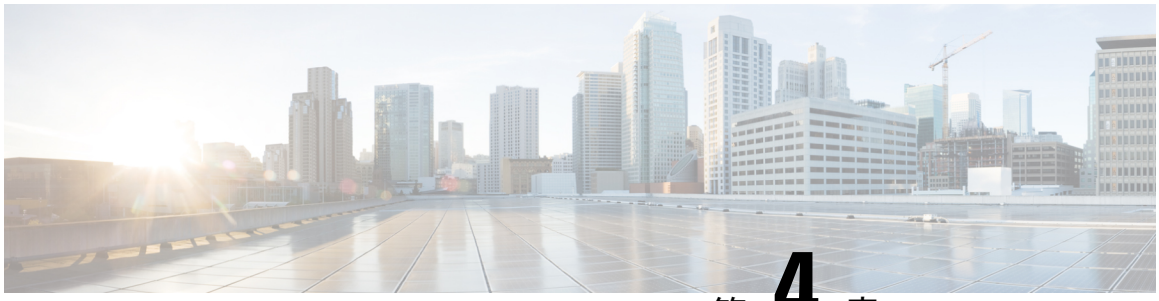
非アクティブ化された製品のサブスクリプション ライセンスは、[アクティベーションの保留（Activation pending）] テーブルに戻されます。

サブスクリプション ライセンスは、新しい製品インスタンスをアクティブ化するために使用できるようになりました。または、既存の製品インスタンスにライセンスを適用することもできます。詳細については、「製品インスタンスのアクティブ化」を参照してください。

製品の非アクティブ化に関する電子メールがエンタープライズ管理者に送信されます。

非アクティブ化プロセスでエラーが発生した場合は、Support Case Manager でシスコサポートチームにお問い合わせください。

[非アクティブ化（Deactivate）] オプションでは、ライセンスのない製品インスタンスまたは外部で管理されている製品インスタンスは削除されません。



第 4 章

ロールベース アクセス コントロールの管理

Security Provisioning and Administration 管理者は、エンタープライズ内のユーザー、グループ、およびロールを管理します。管理者は、一元化された場所から、新しいユーザーの招待、アカウントの無効化、ユーザーグループの編成、エンタープライズ内のすべての製品のユーザーアクセスロールの管理を行うことができます。

• アクティビティログの表示 （48 ページ）

エンタープライズにおけるロールベースのアクセス制御

Security Provisioning and Administration は、エンタープライズ全体のアクセス管理を自動化するロールベースアクセスコントロール（RBAC）をサポートしています。ロールは、製品内の機能へのユーザーアクセスのレベルを定義します。Security Provisioning and Administration を使用すると、エンタープライズ内のユーザーロールの管理を一元化できます。これにより、エンタープライズユーザーは、繰り返しログインすることなく製品をシームレスに切り替えることができます。

エンタープライズ管理者は、製品に適用可能なユーザーロールを定義し、各ユーザーに1つ以上のロールを割り当てることができます。ユーザーアカウントは、グループと呼ばれる管理可能な単位に編成できます。これにより、複数のユーザーに同時にロールを割り当てることができます。各グループには1つ以上のロールを割り当てることができ、グループのメンバーはそれらのロールを継承します。

Security Provisioning and Administration ユーザーインターフェイスには、ユーザー、グループ、およびロールを管理するための個別のページがあります。

[ユーザー（Users）] ページからは、次の操作が行えます。	[グループ（Groups）] ページからは、次の操作が行えます。	[ロール（Roles）] ページからは、次の操作が行えます。
• ユーザーの作成 • ユーザーにロールを割り当てる • グループへのユーザーの追加 • ユーザーの名前の編集 • ユーザーアカウントの無効化 • ユーザーアカウントの復元 • ユーザーのリストの表示 • 名前、タイプ、またはステータスに基づいてユーザーを検索する ユーザーアカウントは、次のステータスに基づいて分離されます。 • [現在のアカウント（Current Accounts）]：このタブには、すべてのアクティブなユーザーが表示されます。 • [保留中の招待（Pending Invitations）]：このタブには、招待され、アクティブ化が保留中のすべてのユーザーが表示されます。 • [無効なアカウント（Disabled Accounts）]：このタブには、アカウントが無効になっているすべてのユーザーが表示されます。	• グループを作成し、グループにユーザーを追加する • グループ名の編集 • ユーザーのグループへの追加または削除 • ロールのグループへの割り当て • グループの削除 • エンタープライズ用に作成されたグループのリストの表示	• 製品に関連付けられているロールのリストの表示 • ユーザーおよびグループへのロールの割り当て • ユーザーまたはグループに割り当てられているロールの編集または削除

ユーザーの管理

- エンタープライズに新しいユーザーを手動で追加するには、「ユーザーの招待」を参照してください。このタスクでは、新しいユーザーをグループに追加してロールを割り当てることができるため、新しいユーザーのオンボーディングに役立ちます。このタスクを使用して、一度に最大 20 人のユーザーを招待できます。
- ユーザーの詳細をエンタープライズにインポートして新しいユーザーを自動的に作成するには、「ユーザーのインポート」を参照してください。このタスクでは、最大20人のユーザーの詳細を含む.csvファイルをアップロードして、ユーザーを追加できます。ファイルがアップロードされたら、それらのユーザーをグループに追加し、ロールを割り当てることができます。
- ユーザーの名前を編集するには、「ユーザー名の編集」を参照してください。
- ユーザーを無効にするには、「ユーザーアカウントの無効化」を参照してください。
- 無効化されたユーザーへのアクセスを復元するには、「ユーザーアカウントの復元」を参照してください。
- エンタープライズからユーザーを削除するには、「ユーザーアカウントの削除」を参照してください。

グループの管理

グループを使用すると、ユーザーアカウントを1つのユニットに編成して、統一されたロールと権限を割り当てることができます。

（注） グループの作成はオプションですが、共通の権限を共有する一連のユーザーを管理する必要がある場合に役立ちます。

- 新しいグループを作成し、グループにメンバーを追加するには、「新規グループの作成」を参照してください。
- グループの名前と説明を編集するには、「グループ名の編集」を参照してください。
- 1つまたは複数のロールをグループに割り当てるには、「ロールのグループへの割り当て」を参照してください。グループ内のすべてのユーザーは、グループロールを継承します。
- エンタープライズ用に作成されたすべてのグループを表示するには、[グループ（Groups）]ページに移動します。[グループ（Groups）]ページには、エンタープライズ内のすべてのグループのリストが表示されます。
- グループからユーザーを削除し、すべてのユーザーが削除された後にグループを削除するには、「グループからユーザーを削除」および「グループの削除」を参照してください。

ロールの管理

Security Provisioning and Administration では、製品インスタンスレベルでロールベースのアクセス制御を有効にします。これにより、各製品インスタンス内のユーザーにロールを割り当てることができ、管理アクセスを正確に制御できます。

次に、ユーザーとグループのロールを割り当てて管理するさまざまな方法を示します。

- エンタープライズにユーザーの招待ときに、新しいユーザーにロールを割り当てます。
- すでにエンタープライズに招待されている新しいユーザーにロールを割り当てます。「ユーザーにロールを割り当てる」を参照してください。
- エンタープライズに参加しているユーザーとグループにロールを割り当てます。「既存のユーザーへのロールの割り当て」を参照してください。
- ロールのグループへの割り当て。このタスクを使用すると、ユーザーのグループにロールを効果的に割り当てることができ、[グループ（Groups）]ページからアクセスできます。
- ロールの割り当てを編集して、ユーザーに割り当てられているロールを変更または削除します。「ロールの割り当ての削除」を参照してください。

重要 このドキュメントに記載されているすべてのタスクは、Security Provisioning and Administration アプリケーションにログインした後にのみ実行されます。

ユーザーの招待

エンタープライズ管理者は、ユーザーをエンタープライズに招待できます。

このタスクでは、新しいユーザーをグループに追加してロールを割り当てることができるため、新しいユーザーのオンボーディングに役立ちます。このタスクを使用して、一度に最大20人のユーザーを招待できます。

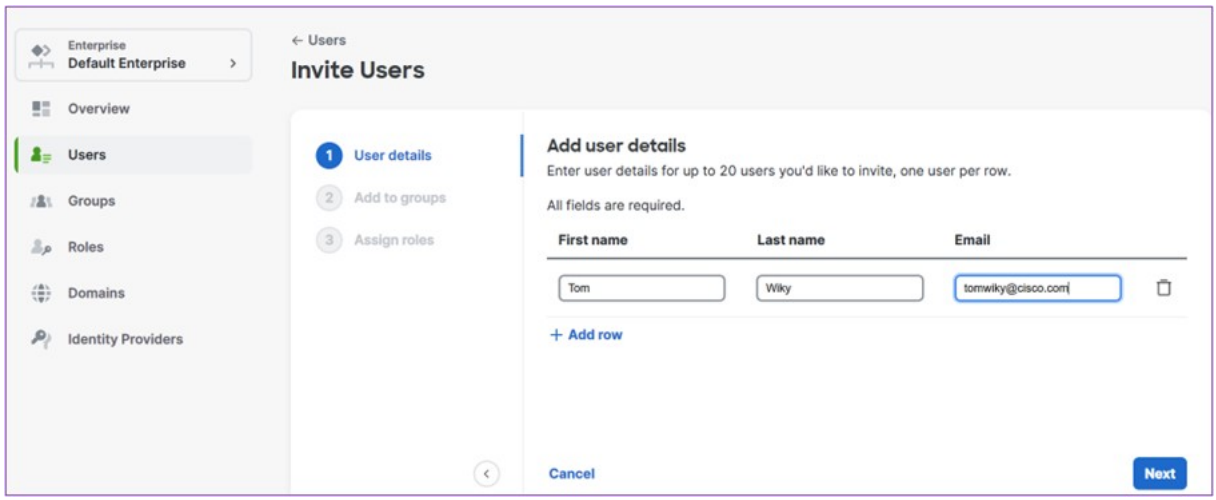
手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー（Users）] ページで、[ユーザーの招待（Invite users）] ボタンをクリックします。

ステップ 3 [ユーザーの詳細の追加（Add user details）]ペインで、ユーザーの名、姓、電子メールアドレスを入力します。

次の手順に進むには、電子メールアドレスを正しい形式で入力したこと、および電子メールアドレスがエンタープライズにまだ存在していないことを確認します。

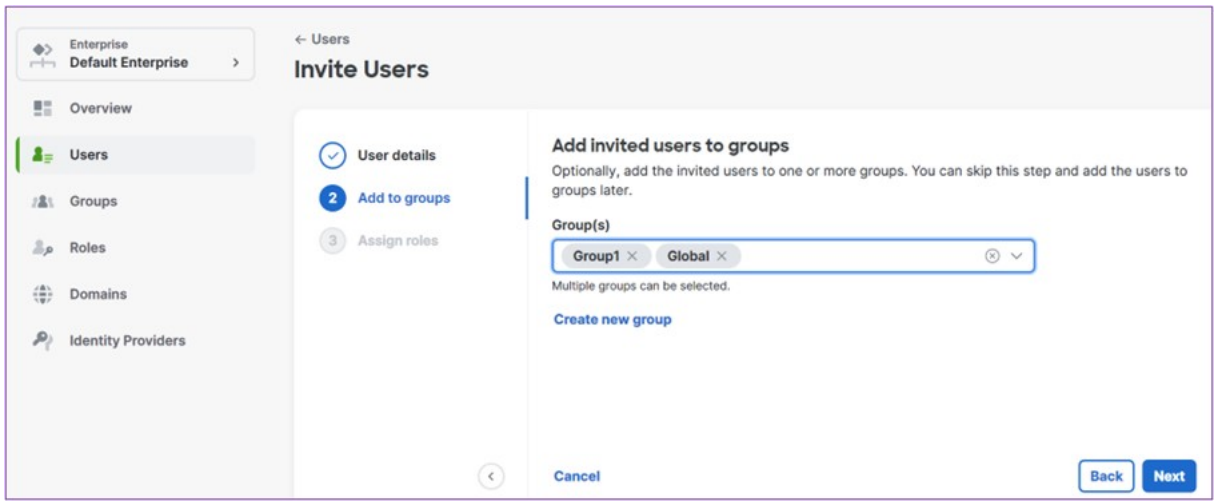


[行の追加（Add row）] オプションを使用して、最大 20 人のユーザーアカウントを追加できます。

ステップ 4 [Next] をクリックします。

この手順により、[グループに追加（Add to groups）] オプションが有効になります。

ステップ 5 （オプション）[招待されたユーザーをグループに追加（Add invited users to groups）] ペインで、[グループ（Group(s)）] ドロップダウンリストから 1 つまたは複数のグループを選択します。これにより、招待されたユーザーを選択したグループに追加できます。



新しいグループを作成し、新しいグループにユーザーを追加できます。

a) 新しいグループを作成するには、[新しいグループの作成（Create new group）] をクリックします。
b) [新しいグループの作成（Create New Group）] スライドインペインで、グループ名と説明を入力します。
c) [グループの作成（Create group）] ボタンをクリックします。

招待されたユーザーが追加されるグループのリストに新しいグループが追加されます。

ステップ 6 [Next] をクリックします。

この手順により、[ロールの割り当て（Assign roles）] オプションが有効になります。

ステップ 7 [招待されたユーザーへのロールの割り当て（Assign role to guests）] ペインで、次の手順を実行します。

a) [割り当てるロール（Roles to assign）] ドロップダウンリストからロールを選択します。

これは、Security Provisioning and Administration がメンバーまたは管理者ロールをユーザーに割り当てるために必須の手順です。

b) 選択したロールをエンタープライズに関連付けるには、[割り当て（Assign within）] ドロップダウンリストから [エンタープライズ（Enterprise）] を選択します。

c) ユーザーに製品ロールを追加するには、[行の追加（Add row）] をクリックします。

1. [割り当てるロール（Roles to assign）] ドロップダウンリストから製品ロールを選択します。
2. [割り当て（Assign within）] ドロップダウンリストから対応する製品インスタンスを選択します。

ステップ 8 [終了して招待（Finish & invite）] をクリックします。

招待されたユーザーには、1 時間で期限切れになるアクティベーションリンクが記載された電子メールが送信されます。

[ユーザー（Users）] ページで、[保留中の招待（Pending inspections）] タブをクリックして、まだアクティブ化されていない招待を表示します。

Security Provisioning and Administration にすでに存在するユーザーを招待した場合、そのユーザーは [ユーザー（Users）] ページの [現在のアカウント（Current Accounts）] タブに表示されます。

ユーザーのインポート

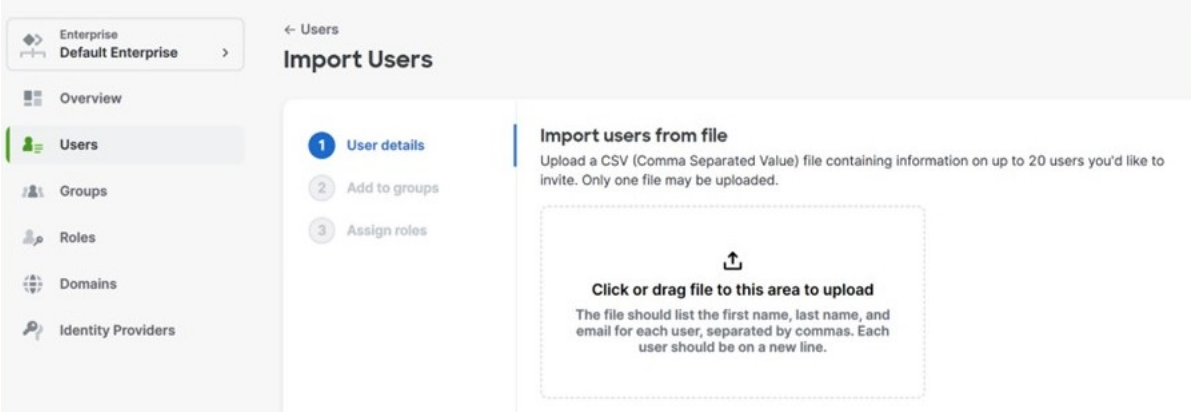
ユーザーの詳細を含むファイルをインポートすることで、複数のユーザーをエンタープライズに招待するプロセスを自動化します。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー（Users）] ページで、[ユーザーのインポート（Import users）] をクリックします。

ステップ 3 [ファイルからのユーザーのインポート（Import users from file）] ペインで、.csv ファイルをアップロードまたはドラッグアンドドロップします。



（注）
.csv ファイルには、次の表に示されているように、各ユーザーの名、姓、および電子メールアドレスが表形式でリストされている必要があります。各ユーザーは 1 行ごとにリストに記載する必要があります。

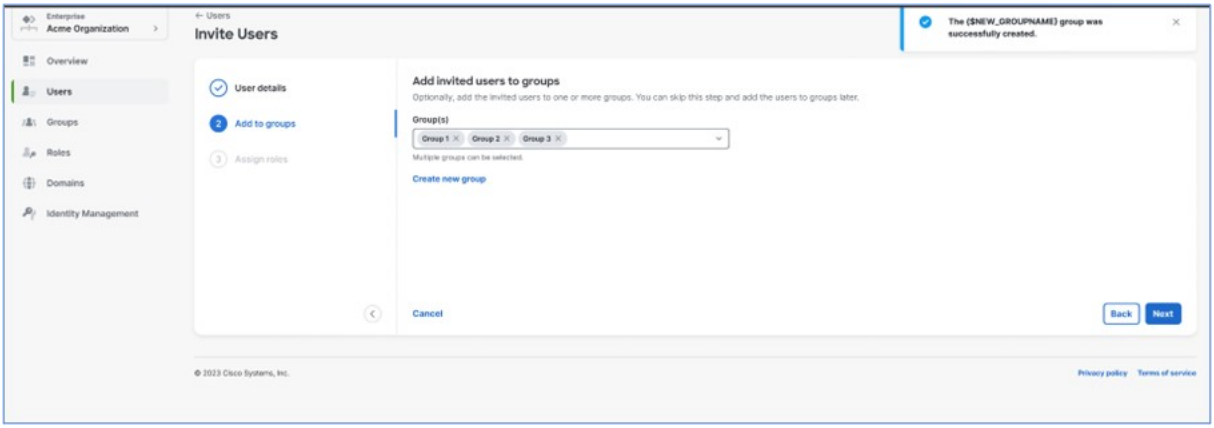
表の最初の行が「firstName」、「lastName」、「email」というタイトルのヘッダーとして機能していることを確認します。後続の行には、ユーザー情報を含める必要があります。

図 *1 : .csv* ファイルの形式

firstName	lastName	email
John	Doe	johndoe@abc.com
Jane	Doe	janeD@abc.com

ファイルが正常にインポートされると、[グループに追加（Add to groups）] オプションが有効になります。

ステップ 4 （オプション）[グループ（Group(s)）] ドロップダウンリストから、招待されたユーザーを追加するグループを選択します。



ステップ 5 [Next] をクリックします。

この手順では、ユーザーにロールを割り当てることができます。

ステップ 6 [招待されたユーザーへのロールの割り当て（Assign role to guests）] ペインで、次の手順を実行します。

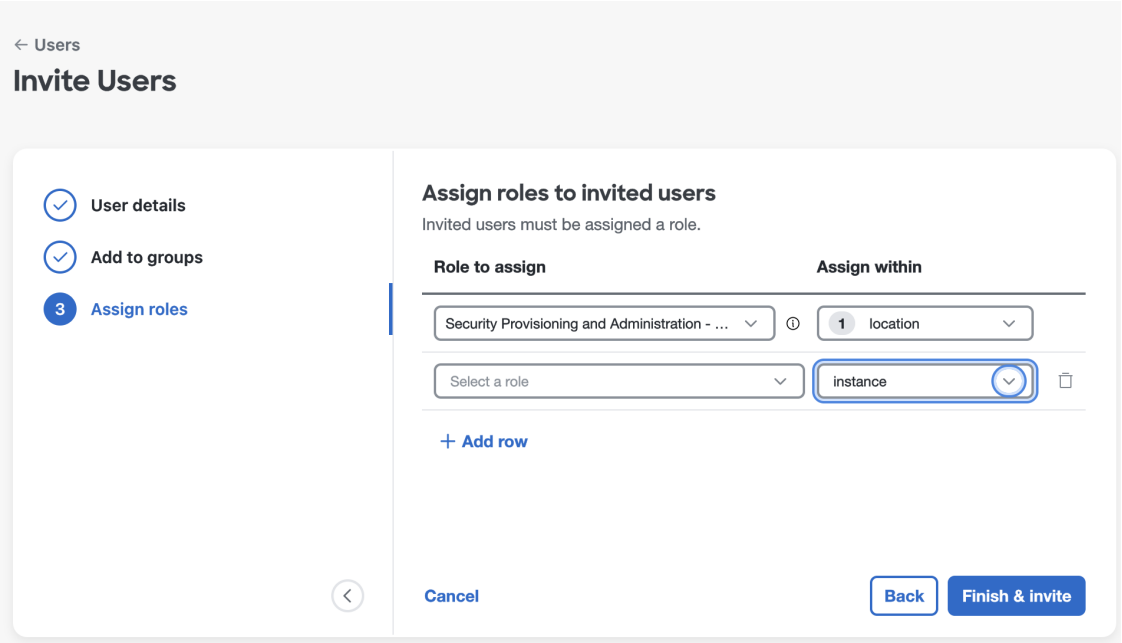
a) [割り当てるロール（Roles to assign）] ドロップダウンリストからロールを選択します。

これは、Security Provisioning and Administration がメンバーまたは管理者ロールをユーザーに割り当てるために必須の手順です。

b) 選択したロールをエンタープライズに関連付けるには、[割り当て（Assign within）] ドロップダウンリストから [エンタープライズ（Enterprise）] を選択します。

c) ユーザーに製品ロールを追加するには、[行の追加（Add row）] をクリックします。

1. [割り当てるロール（Roles to assign）] ドロップダウンリストから製品ロールを選択します。
2. [割り当て（Assign within）] ドロップダウンリストから対応する製品インスタンスを選択します。



ステップ 7 [終了して招待（Finish & invite）] をクリックします。

招待されたユーザーには、1 時間で期限切れになるアクティベーションリンクが記載された電子メールが送信されます。

[ユーザー（Users）] ページで、[保留中の招待（Pending inspections）] タブをクリックして、まだアクティブ化されていない招待を表示します。

Security Provisioning and Administration に存在するユーザーを招待した場合、そのユーザーは [現在のアカウント（Current Accounts）] タブに表示されます。

ユーザーの表示または検索

[ユーザー（Users）] ページには、エンタープライズ内のユーザーのリストが表示されます。

[ユーザー（Users）]ページの各タブには、ユーザーのタイプ、ステータス、または名前に基づいてユーザーを検索するための検索バーがあります。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

デフォルトでは、[現在のアカウント（Current Accounts）] タブに、エンタープライズ内のすべてのユーザーのリストが表示されます。ユーザーごとに、名前、タイプ、およびステータスが表示されます。

ステップ 2 [保留中の招待（Pending Invitations）] タブをクリックして、アカウントのアクティブ化が保留中のユーザーのリストを表示します。

この段階では、ユーザーは [ステージング（Staged）] または [プロビジョニング済み（Provisioned）] ステータスになっている可能性があります。

ステップ 3 [現在のアカウント（Current Accounts）] タブをクリックして、エンタープライズ内のアクティブユーザーのリストを表示します。

ステップ 4 [無効なアカウント（Disabled Accounts）] タブをクリックして、アカウントがロックアウトまたは一時停止されているユーザーのリストを表示します。

[ロックアウト（Locked out）] または [エンタープライズ無効（Enterprise disabled）] 状態のユーザーの場合、管理者はユーザーへのアクセスを復元する必要があります。[一時停止（Suspended）] または [プロビジョニング解除（Deprovisioned）] 状態のユーザーは、エンタープライズにアクセスできません。

ユーザー名の編集

エンタープライズ管理者は、ユーザーの姓名を編集できますが、ユーザーの電子メールアドレスは変更できません。

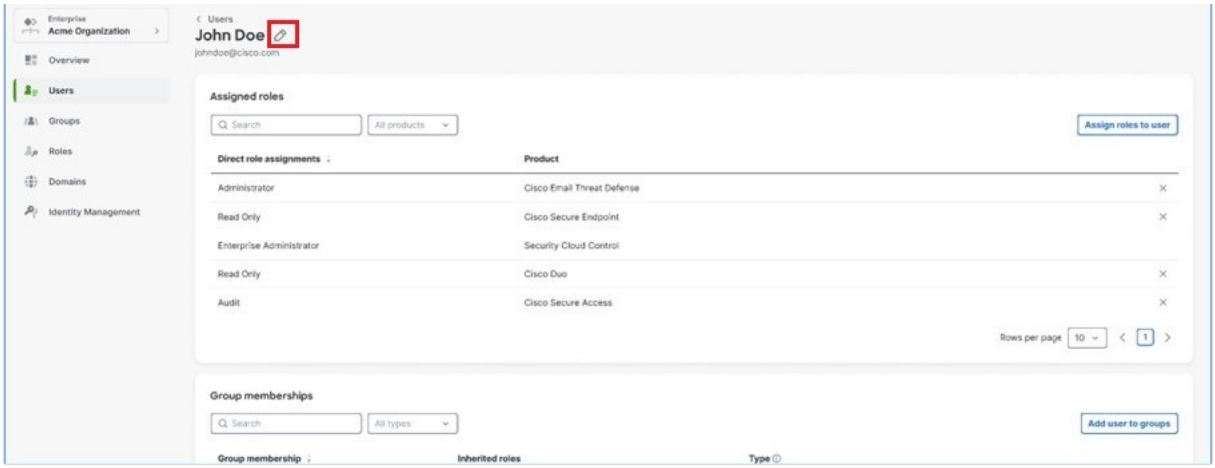
手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

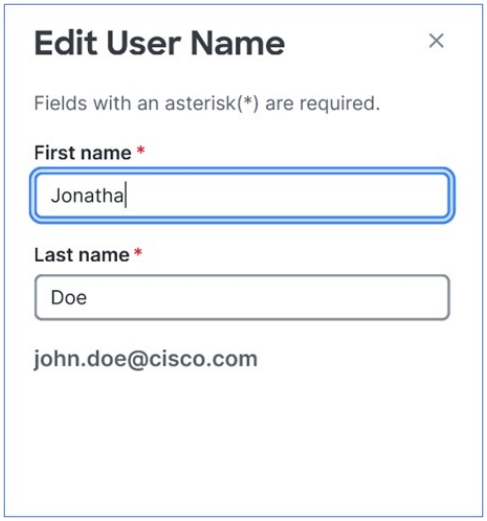
ステップ 2 [ユーザー（Users）] ページで、[現在のアカウント（Current accounts）] タブをクリックします。

ステップ 3 詳細を追加するユーザーの横にある その他メニュー アイコン [...] をクリックし、[詳細の表示（Show Details）] を選択します。

ステップ 4 表示されるページの上部にあるユーザー名の横にある鉛筆アイコンをクリックします。



ステップ 5 [ユーザー名の編集（Edit User Name）] ペインで、必要に応じて名前を編集します。



ステップ 6 **[更新（Update）]**をクリックします。

編集した内容は、[ユーザー（Users）] ページで更新されます。

ユーザーにロールを割り当てる

エンタープライズ管理者は、ユーザーに 1 つ以上のロールを割り当てることができます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー（Users）] ページで、[現在のアカウント（Current accounts）] タブをクリックします。

ステップ 3 編集するユーザーの横にある その他メニュー アイコン  をクリックし、[編集（Edit）] を選択します。

ステップ 4 ページの右上隅にある [ユーザーにロールを割り当てる（Assign role to user）] ボタンをクリックします。

ステップ 5 [ロールの割り当て（Assign Roles）] スライドインペインで、次の手順を実行します。

a) [製品とロール（Product and role）] ドロップダウンリストから、製品に対するユーザーのロールを選択します。

b) [製品インスタンス（Product Instance）] ドロップダウンリストで、選択したロールを割り当てる製品インスタンスを選択します。

選択したロールに対して複数の製品インスタンスを選択できます。

（注）
[製品インスタンス（Product Instance）] ドロップダウンリストで [すべて選択（Select All）] を選択すると、選択したロールはすべての製品インスタンスに割り当てられます。製品の新しいインスタンスが後でエンタープライズに追加された場合、選択したロールは新しい製品インスタンスに自動的に適用されません。新しいインスタンスでロールを割り当てるには、このタスクを繰り返す必要があります。

[行の追加（Add row）] をクリックして、各製品インスタンスにユーザーロールを追加します。

（注）
ユーザーには、特定の製品に対して複数のロールを割り当てることができます。

ステップ 6 [ロールの割り当て（Assign roles）] をクリックします。

選択した製品ロールが対応するユーザーに割り当てられます。

グループへのユーザーの追加

エンタープライズ管理者は、ユーザーをグループに追加できます。ユーザーはグループのロールを継承します。

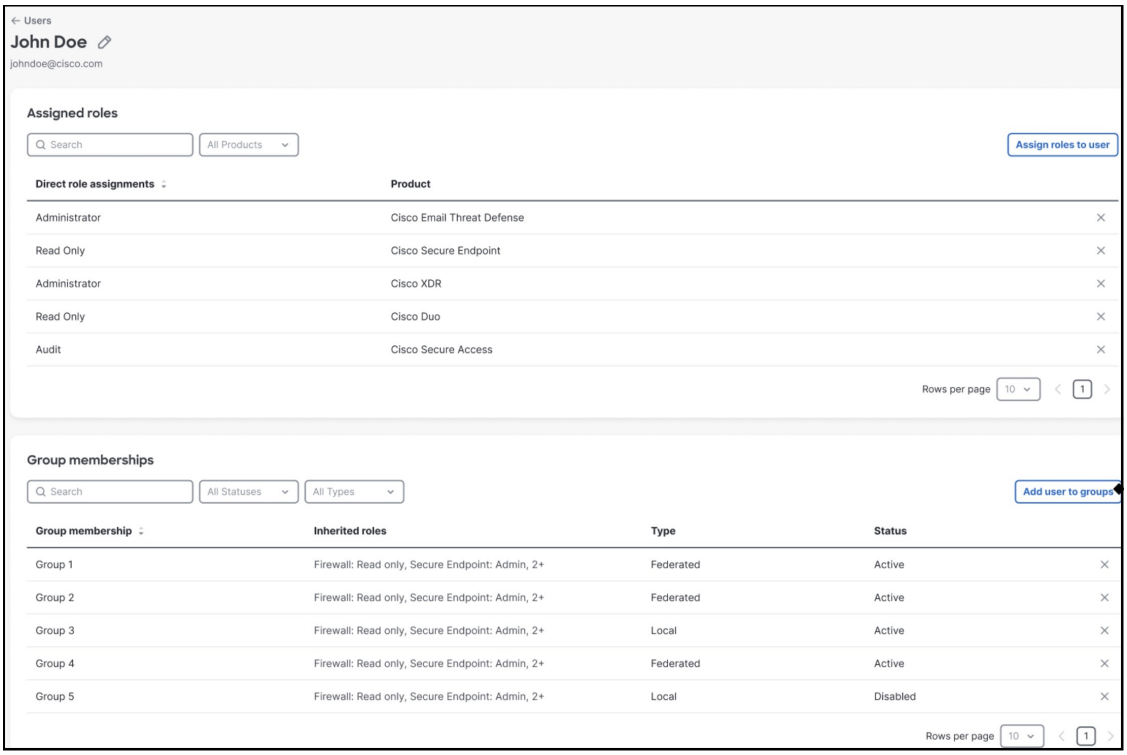
手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー（Users）] ページで、[現在のアカウント（Current accounts）] タブをクリックします。

ステップ 3 詳細を追加するユーザーの横にある その他メニュー アイコン [...] をクリックし、[編集（Edit）] を選択します。

ステップ 4 [グループメンバーシップ（Group Memberships）] セクションで、[ユーザーをグループに追加（Add user to groups）] ボタンをクリックします。



ステップ 5 [グループに追加（Add to Groups）] スライドインペインで、[グループ（Group(s)）] ドロップダウンリストから関連するグループを選択します。

（注）
1 人のユーザーに複数のグループを割り当てることができます。

ステップ 6 [グループに追加（Add to Groups）] をクリックします。

既存のユーザーへのロールの割り当て

ロールを使用すると、事前定義された権限をユーザーまたはグループに割り当てることができます。管理者は、1 つ以上のユーザーまたはグループに複数のロールを割り当てることができます。

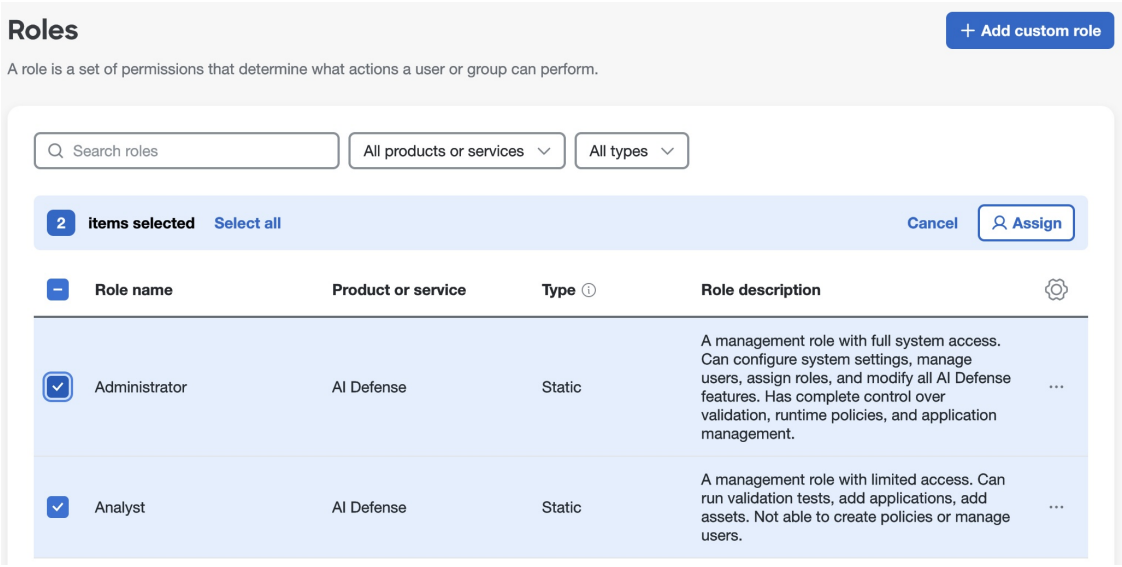
手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ロール（Roles）] をクリックします。

[ロール（Roles）] ページには、名前、所属する製品、およびロールの説明を含むロールのリストが表示されます。

ステップ 2 [ロール（Roles）] ページで、ロール名の横にあるチェックボックスをオンにして、割り当てるロールを選択します。

（注）
複数のロールをユーザーとグループに割り当てることができます。



ステップ 3 [割り当て（**Assign**）] をクリックします。

ステップ 4 [ロールの割り当て（Assign role）] スライドインペインで、次の手順を実行します。

a) 選択した製品ロールを割り当てる場所を選択します。

b) [ユーザー（Users）] および [グループ（Groups）] ドロップダウンリストから、それぞれユーザーとグループを選択します。

ステップ 5 [ロールの割り当て（Assign role）] をクリックします。

選択したロールが、選択したユーザーおよびグループに割り当てられます。

ロールの割り当ての削除

エンタープライズ管理者は、ユーザーおよびグループに割り当てられているロールを割り当てたり、割り当て解除したりできます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ロール（Roles）] をクリックします。

ステップ 2 [ロール（Roles）] ページで、削除するロールの横にある その他メニュー アイコン  をクリックし、[詳細の表示（Show Details）] を選択します。

結果のページには、選択したロールが割り当てられているすべてのユーザーとグループが表示されます。

ステップ 3 選択したロールとユーザーまたはグループの関連付けを解除するには、ユーザーまたはグループの横にある X アイコンをクリックします。

a) 確認ダイアログボックスで [削除（Remove）] をクリックします。

ユーザーまたはグループには、削除されたロールの権限がありません。

カスタムロールの作成

エンタープライズ管理者は、特定の権限を持つカスタムロールを作成できます。

始める前に

カスタムロールを作成する前に、次の点に注意してください。

- カスタムロールがサポートされていない製品のカスタムロールは作成できません。
- 製品のカスタムロールを作成していて、後でその製品がプロビジョニング解除された場合、その製品のカスタムロールは非表示になりますが、削除はされません。製品が再度アクティブ化されると、その製品のカスタムロールを割り当てに使用できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ロール（Roles）] をクリックします。

[ロール（Roles）] ページには、名前、所属する製品、タイプ、およびロールの説明を含むロールのリストが表示されます。

ステップ 2 [ロール（Roles）] ページで、[カスタムロールの追加（Add Custom Role）] をクリックします。

ステップ 3 [カスタムロールの追加（Add Custom Role）] ページの [ロールの詳細（Role Details）] セクションで、次の手順を実行します。

a) [製品（Product）] ドロップダウンリストからロールの製品を選択します。

b) [ロール名（Role Name）] フィールドに、ロールの名前を入力します。

（注）
- ロールの名前は 50 文字までに制限されています。ロール名には英数字、ハイフン、下線を使用できます。その他の文字は使用できません。
- 特定の製品に対して同じ名前の 2 つのカスタムロールは設定できません。

c) （任意）ロールの説明を入力します。

d) [次へ（Next）] をクリックします。このステップで、ロールの権限を指定できます。

ステップ 4 [カスタムロールの追加（Add Custom Role）] ページの [権限の詳細（Permission Details）] セクションで、次の手順を実行します。

a) 表示されている権限のリストから権限を選択します。

b) [次へ（Next）] をクリックします。

ステップ 5 [概要（Summary）] セクションで、カスタムロールの詳細を確認します。

カスタムロールの追加に進むには、[ロールの作成（Create Role）] をクリックします。

ロールの詳細を変更するには、[戻る（Back）] をクリックして、必要な編集を加えます。

カスタムロールを追加せずに続行するには、[キャンセル（Cancel）] をクリックします。

カスタムロールは作成されると、[ロール（Roles）] ページのロールリストに追加されます。

カスタムロールの編集

カスタムロールを編集する前に、そのロールがユーザーに割り当てられているか確認してください。カスタムロールに編集を加えると、製品へのユーザーアクセスにすぐに影響を及ぼします。

カスタムロールの名前と権限のみを編集でき、カスタムロールを適用する製品は変更できません。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ロール（Roles）] をクリックします。

[ロール（Roles）] ページには、名前、所属する製品、タイプ、およびロールの説明を含むロールのリストが表示されます。

ステップ 2 [ロール（Roles）]ページで、カスタムロールの横にある その他メニュー  をクリックし、[編集（Edit）] を選択します。

または、カスタムロールの横にある その他メニュー  をクリックし、[詳細の表示（Show Details）] を選択します。

[ロールの詳細（Role Details）] ページで、[編集（Edit）] をクリックします。

（注）
[編集（Edit）] ボタンは、カスタムロールの場合にのみ表示されます（静的ロールは編集できません）。

ステップ 3 [カスタムロールの編集（Edit Custom Role）]ページで、カスタムロールの名前と説明に必要な編集を加え、[次へ（Next）] をクリックします。

ステップ 4 [カスタムロールの編集（Edit Custom Role）] ページの [権限の詳細（Permission Details）] セクションで、該当する権限を選択して [次へ（Next）] をクリックします。

ステップ 5 [概要（Summary）] セクションで、カスタムロールの詳細を確認します。

ロールの詳細を変更するには、[戻る（Back）] をクリックして、必要な編集を加えます。

加えた変更を更新するには、[変更の保存（Save Changes）] をクリックします。

変更をキャンセルして更新しない場合は、[キャンセル（Cancel）] をクリックします。

カスタムロールを編集すると、[ロール（Roles）] ページのロールリストが更新されます。

カスタムロールの削除

カスタムロールは、ユーザーやグループに割り当てられていない場合にのみ削除できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ロール（Roles）] をクリックします。

[ロール（Roles）] ページには、名前、所属する製品、タイプ、およびロールの説明を含むロールのリストが表示されます。

ステップ 2 削除メニューにアクセスするには、次のいずれかを実行します。

- [ロール（Roles）] ページで、カスタムロールの横にある その他メニュー  をクリックし、[削除（Delete）] を選択します。
- [ロール（Roles）] ページで、カスタムロールの横にある その他メニュー  をクリックし、[詳細の表示（Show Details）] を選択します。

[ロールの詳細（Role Details）] ページで、[削除（Delete）] ボタンをクリックします。

- [ロール（Roles）] ページでロールに対するチェックボックスをオンにし、上部のバーにある [削除（Delete）] ボタンをクリックします。

（注）
[削除（Delete）] ボタンは、カスタムロールの場合にのみ表示されます（静的ロールは削除できません）。

ロールがユーザーやグループにすでに割り当てられている場合、警告メッセージが表示され、ロールは削除されません。

ステップ 3 [カスタムロールの削除（Delete Custom Role）] 確認ダイアログボックスで、[削除（Delete）] をクリックします。

多要素認証設定のリセット

企業が Security Cloud Sign On で認証するために Duo 多要素認証（MFA）を使用している場合は、ユーザーの Duo MFA 設定をリセットできます。リセットすると、ユーザーの MFA ログイン情報が削除され、ユーザーは新しい認証要素とログイン情報を設定できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [現在のユーザー（Current Users）] タブで、ユーザーを見つけます。

ステップ 3 ユーザーの その他メニュー アイコン  をクリックし、[MFAのリセット（Reset MFA）] を選択します。

ステップ 4 確認ダイアログボックスで [MFAのリセット（Reset MFA）] をクリックします。

次回のサインイン時に、そのユーザーは Duo MFA のログイン情報と認証要素を設定するように求められます。

ユーザーパスワードのリセット

エンタープライズ管理者は、ドメインの要求および検証に属するユーザーのパスワードをリセットできます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [現在のアカウント（Current Accounts）] で、パスワードをリセットするユーザーを見つけ、その他メニューアイコン をクリックします。

ステップ 3 ドロップダウンメニューで、[パスワードのリセット（Reset password）] をクリックします。

確認ダイアログボックスで、[パスワードのリセット（Reset password）] をクリックします。

次回のサインイン時に、そのユーザーはパスワードをリセットするよう求められます。

ユーザーアカウントの無効化

エンタープライズ管理者は、ユーザーアカウントを無効できます。無効化されたユーザーアカウントは、すべてのアクセス権限を失います。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー（Users）] ページで、[現在のアカウント（Current accounts）] タブをクリックします。

ステップ 3 ユーザー名の横にあるその他メニューアイコン をクリックし、[アカウントの無効化（Disable account）] を選択します。

ステップ 4 表示されるダイアログボックスで、[アカウントの無効化（Disable account）] をクリックします。

ユーザーアカウントは、[ユーザー（Users）] ページの [無効なアカウント（Disabled Accounts）] タブに表示されます。

ユーザーアカウントの復元

エンタープライズ管理者は、無効化されたユーザーアカウントを復元できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [ユーザー（Users）] ページで、[無効なアカウント（Disabled Accounts）] タブをクリックします。

ステップ 3 ユーザー名の横にある その他メニュー アイコン をクリックし、[アクセスの復元（Restore access）] を選択します。

ステップ 4 表示されるダイアログボックスで、[アクセスの復元（Restore access）] をクリックします。

ユーザーが以前に関連付けられていたすべてのグループとロールを含むユーザーアクセスが復元されます。ユーザーは、[ユーザー（Users）] ページの [現在のアカウント（Current Accounts）] タブに表示されます。

ユーザーアカウントの削除

エンタープライズ管理者は、エンタープライズからユーザーアカウントを削除できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ユーザー（Users）] をクリックします。

ステップ 2 [現在のアカウント（Current Accounts）] タブで、削除するユーザーエントリの横にあるその他メニュー をクリックし、[ユーザーの削除（Remove user）] を選択します。

ステップ 3 [ユーザーの削除（Remove User）] ダイアログボックスで、[削除（Remove）] をクリックします。

ユーザーアカウントがエンタープライズから削除され、ユーザーはエンタープライズ内のどの製品にもアクセスできなくなります。

新規グループの作成

エンタープライズ管理者は、グループを作成し、そのグループにユーザーを追加できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[グループ（Groups）] をクリックします。

ステップ 2 [グループ（Groups）] ページで、[グループの追加（Add group）] をクリックします。

ステップ 3 [名前（Name）] フィールドおよび [説明（Description）] フィールドに詳細を入力します。

（注）
グループ名は 50 文字を超えないようにしてください。

ステップ 4 [Next] をクリックします。

ステップ 5 （オプション）グループにユーザーを追加するには、[ユーザーの追加（Add users）] ドロップダウンリストからユーザーを選択します。

ステップ 6 [終了（Finish）] をクリックします。

新しいグループが [グループ（Groups）] ページに表示されます。

グループ名の編集

エンタープライズ管理者は、グループの名前と説明を変更できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[グループ（Groups）] をクリックします。

ステップ 2 [グループ（Groups）] ページで、編集するグループの横にある その他メニュー アイコン  をクリックし、[編集（Edit）] オプションを選択します。

ステップ 3 [グループ（Groups）] ページで、鉛筆アイコンをクリックしてグループ名を編集します。

ステップ 4 [グループ名の編集（Edit Group Name）] スライドインペインで、グループの名前と説明を編集します。

ステップ 5 **[更新（Update）]**をクリックします。

グループ名の更新は、[グループ（Groups）] ページで確認できます。

グループへのユーザーの追加

エンタープライズ管理者は、グループにユーザーを追加できます。

手順

ステップ 1 **[管理者アクセス制御（Administrator Access Control）] > [管理者グループ（Admin Groups）]**を選択します。

ステップ 2 [Security Provisioning and Administration] ナビゲーションメニューで、[グループ（Groups）] をクリックします。

ステップ 3 [グループ（Groups）] リストページで、ユーザーを追加するグループの横にあるその他メニューのアイコン  をクリックし、[詳細の表示（Show Details）] オプションを選択します。

ステップ 4 [ユーザー（User）] セクションで [ユーザーの追加（Add Users）] をクリックします。

ステップ 5 表示されるダイアログボックスの [ユーザーの追加（Add Users）] ドロップダウンリストから、このグループに追加するユーザーを選択します。

ステップ 6 [ユーザの追加（Add Users）] をクリックします。

新しく追加されたユーザーは、[グループ（Groups）] ページの [ユーザー（Users）] セクションに一覧表示されます。

ロールのグループへの割り当て

エンタープライズ管理者は、ユーザーおよびグループに1つ以上のロールを割り当てることができます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[グループ（Groups）] をクリックします。

ステップ 2 [グループ（Groups）] ページで、グループの横にある その他メニュー アイコン  をクリックし、[詳細の表示（Show Details）] オプションを選択します。

ステップ 3 [グループ（Groups）]ページの [割り当て済みロール（Assigned Roles）] セクションで、[ロールの割り当て（Assign role）] ボタンをクリックします。

ステップ 4 [ロールの割り当て（Assign Roles）] スライドインペインで、次の手順を実行します。

（注）

グループには、製品に対して複数のロールを割り当てることができます。

a) [製品とロール（Product and role）] ドロップダウンリストからロールを選択します。
b) [製品インスタンス（Product Instance）] ドロップダウンリストで、選択したロールを割り当てる製品インスタンスを選択します。

選択したロールを複数の製品インスタンスに割り当てることを選択できます。

ステップ 5 [ロールの割り当て（Assign roles）] をクリックします。

新しく割り当てられたロールは、[グループ（Groups）] ページの [割り当てられたロール（Assigned Roles）] セクションに表示されます。

グループからユーザーを削除

エンタープライズ管理者は、グループからユーザーを削除できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[グループ（Groups）] をクリックします。

ステップ 2 [グループ（Groups）] ページで、ユーザーを削除するグループの横にあるその他メニューのアイコン ... をクリックし、[詳細の表示（Show Details）] オプションを選択します。

ステップ 3 選択したグループのユーザーのリストから、削除するユーザーを選択します。

ステップ 4 [ユーザーの削除（Remove users）] ボタンをクリックします。

表示される確認ダイアログボックスで、[ユーザーの削除（Remove users）] をクリックしてアクションを確認します。

ユーザーがグループから削除されると、[グループ（Groups）] ページのユーザーリストにそのユーザーが表示されなくなります。

グループの削除

グループは、メンバーがいない場合にのみ削除できます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[グループ（Groups）] をクリックします。

ステップ 2 削除するグループの横にある その他メニュー アイコン  をクリックし、[削除（Delete）] を選択します。

ステップ 3 [グループの削除（Delete Group）] 確認ダイアログボックスで [削除（Delete）] をクリックします。

エンタープライズからグループが削除されます。

アクティビティログの表示

管理者は、エンタープライズ内のユーザーログインアクティビティを確認できます。ユーザーログインの詳細は、フィルタリングオプション付きの表形式で表示されます。ユーザーは、日付と時間の範囲、ユーザー、イベントサブタイプなどの条件に基づいて、特定のイベントをフィルタ処理して検索できます。デフォルトでは、直近90日間のアクティビティデータがテーブルに表示されます。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[アクティビティログ（Activity Log）] をクリックします。

[アクティビティログ（Activity Log）] ページには、イベントのリスト、およびデータ、時間、ユーザーの電子メールアドレス、イベント概要などの詳細が表示されます。

ステップ 2 特定のイベントを検索するには、[フィルタ（Filters）] をクリックします。

a) [イベントのフィルタ処理（Filter events）] スライドインペインで、イベントのリストをフィルタ処理する条件を選択します。

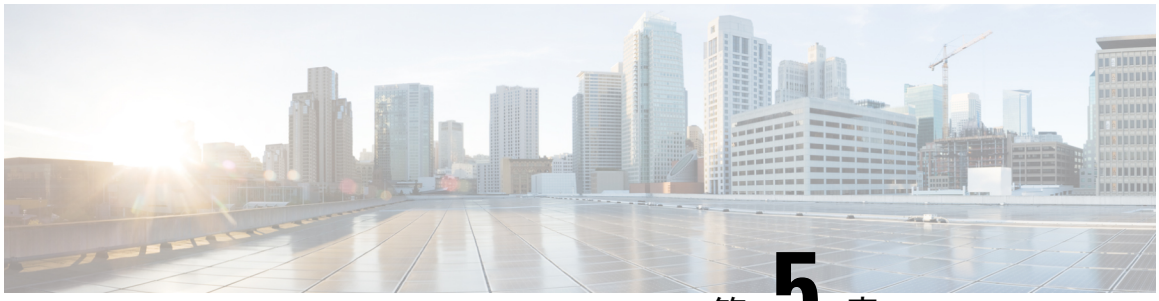
日付と時間の範囲、イベントサブタイプ、またはユーザーを条件に指定でき、条件の組み合わせも選択できます。

b) [イベントのフィルタ処理（Filter events）] をクリックします。

このページには、検索条件に基づいてすべてのイベントが表示されます。

ステップ 3 フィルタを削除してイベントの全リストを表示するには、[すべてリセット（Reset all）] をクリックします。

ステップ 4 最新のイベントのセットを表示するには、[イベントデータの更新（Refresh event data）] をクリックします。このアクションにより、現在のフィルタが適用され、最新のデータが表示されます。



第 5 章

スマートアカウントの接続

Security Provisioning and Administration には、通常はクラウド SaaS サブスクリプションから派生するプラットフォームレベルのサービスを有効にするスマートアカウントを接続するオプションがあります。

スマート アカウント ライセンス

Security Provisioning and Administration 内でスマートアカウントをエンタープライズにリンクできます。スマートアカウントは、アカウント内のスマート セキュリティ ライセンスに基づいてリンクされ、期限日は最も遠い未来の日に設定されます。たとえば、スマートアカウント A で、以下の日付がスマートライセンスの終了日である場合、スマートライセンス 3 を使用して Security Provisioning and Administration との接続を維持し、スマートアカウントの有効性も維持します。

- スマートライセンス 1：終了日 2025 年 1 月 1 日
- スマートライセンス 2：終了日 2025 年 12 月 1 日
- スマートライセンス 3：終了日 2026 年 1 月 1 日

アクティブな Software-as-a-Service（SaaS）ライセンスがなく、スマートライセンスがあるスマートアカウントがエンタープライズにリンクされている場合、プラットフォームサービスが有効になります。

リンクされたスマート アカウント ライセンスの基盤となるすべてのライセンスが非アクティブになっていて、他の SaaS 製品やスマートアカウントの関連付けがない場合、Security Provisioning and Administration は有効なライセンスが適用されるまで、有効なサービスを非アクティブにします。

ユーザーは、エンタープライズにリンクするスマートアカウントの管理者である必要があります。また、エンタープライズにリンクする前に、スマートアカウントに 1 つ以上のアクティブなセキュリティ製品ライセンスが必要です。

（注）
- アクティブなスマートアカウントの有効期限が切れると、スマートアカウントのステータスは [期限切れ（Expired）] に設定されます
- スマートアカウントへのリンクは、アカウント内にアクティブな該当するスマートライセンスが存在する限り維持されます。このリンクは、スマートアカウントを削除した場合、またはスマートアカウントにアクティブなスマートライセンスがない場合は解除されます。
- リンクされたスマートアカウントに関連付けられているスマートライセンスが期限切れになるか、削除された場合、アクティブなスマートライセンスが検索されて、スマートアカウントへのリンクが維持されます。

スマートアカウントのリンク

アクティブなスマートアカウントをエンタープライズにリンクできます。スマートアカウントをリンクする前に、スマートアカウント内の関連するセキュリティライセンスがスキャンされ、将来の期限日が最新のライセンスを使用してアカウントのアクティブなライセンスステータスが検証されます。スマートアカウントはアクティブであると判断された場合、エンタープライズに追加されます。

始める前に

- 次の条件を満たしている場合、スマートアカウントをエンタープライズにリンクできます。
  - スマートアカウントの管理者権限が必要です。
  - スマートアカウントには、1 つ以上のアクティブなセキュリティ製品ライセンスが含まれている必要があります。

手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、**[製品サブスクリプション（Product Subscriptions）]** > **[スマート アカウント ライセンス（Smart Accounts Licensing）]** をクリックします。

ステップ 2 [スマート アカウント ライセンス（Smart Account Licensing）] ペインで、[スマート アカウント ライセンスのリンク（Link Smart Accounts Licensing）] をクリックします。

a) 最初のアクセスでは、Cisco Customer Identity（CCI）アカウントへのログインを求められます。

CCI による認証が成功すると、次のステップに進むことができます。

b) 後続のアクセスでは、CCI トークンがまだ有効ならば、ログインは求められません。

CCI トークンは、4 ～ 12 時間の期間で期限切れになります。

別のユーザーとしてログインするには、CCI トークンが期限切れになるまで待ちます。

ステップ 3 [スマート アカウント ライセンスのリンク（Link Smart Accounts Licensing）] スライドインペインで、[スマートアカウント（Smart accounts）] リストからエンタープライズに追加する 1 つまたは複数のアカウントを選択します。

a) または、[すべて選択（Select All）] チェックボックスをオンにして、すべてのアカウントを追加します。

a) [Add] をクリックします。

選択したアカウントが追加され、[スマート アカウント ライセンス（Smart Accounts Licensing）] ページに表示されます。スマートアカウントには、ステータス、期限日、および最後に同期された日付が表示されます。スマートライセンスのステータスは 24 時間ごとに 1 回更新されます。

スマートアカウントの削除

エンタープライズからスマート アカウント ライセンスをリンク解除または削除できます。スマートアカウントを削除すると、すべてのスマート アカウント ライセンスが削除されます。

（注） 残っている唯一のアクティブなスマートアカウントを削除し、エンタープライズに関連付けられている他の SaaS トライアルやサブスクリプションがない場合、そのエンタープライズは「ライセンスなし」の状態に移行します。これは、エンタープライズの基礎となるプラットフォームサービスに影響を与える可能性があります。

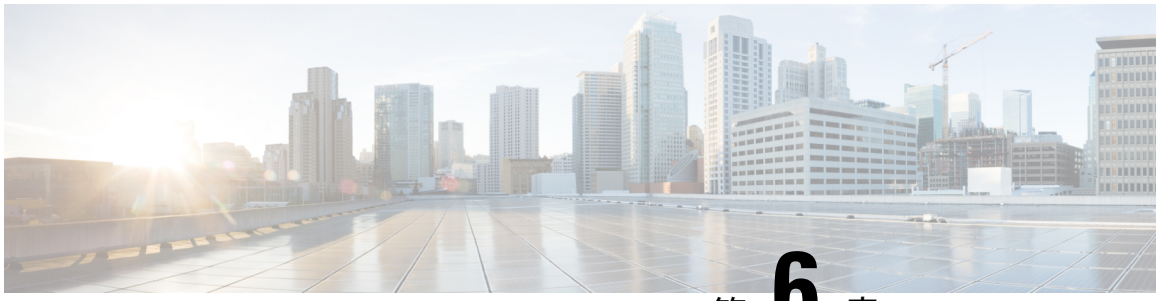
手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、**[製品サブスクリプション（Product Subscriptions）] > [スマート アカウント ライセンス（Smart Accounts Licensing）]** をクリックします。

ステップ 2 [スマート アカウント ライセンス（Smart Account Licensing）] ペインで、削除するスマートアカウントの横にある削除アイコンをクリックします。

ステップ 3 [スマートアカウントの削除（Remove Smart Account）] ダイアログボックスで [削除（Delete）] をクリックします。

スマートアカウントがエンタープライズから削除されます。



第 6 章

ドメインの管理

Security Provisioning and Administration で エンタープライズ のドメインの要求および検証できます。これは、ID プロバイダー統合ガイドための前提条件です。また、エンタープライズ 管理者が要求されたドメインでユーザーのパスワードまたは MFA 設定をリセットできるようにするためにも必要です。

ドメインの要求および検証

- 作成した DNS レコードは、Security Provisioning and Administration がドメインを検証したら削除できます。
- 現在、Security Provisioning and Administration を使用して単一のドメインを検証できます。複数のドメインを検証する必要がある場合、Cisco Technical Assistance Center（Cisco TAC）でケースを開いてください。

始める前に

このタスクを完了するには、ドメインのレジストラサービスでドメインネームシステム（DNS）レコードを作成できる必要があります。

[ドメイン（Domains）] タブには、検証済みまたは検証中のドメインが一覧表示されます。ドメインを要求済みでない場合は、代わりに [+ドメインの追加（+ Add Domain）] ボタンが表示されます。

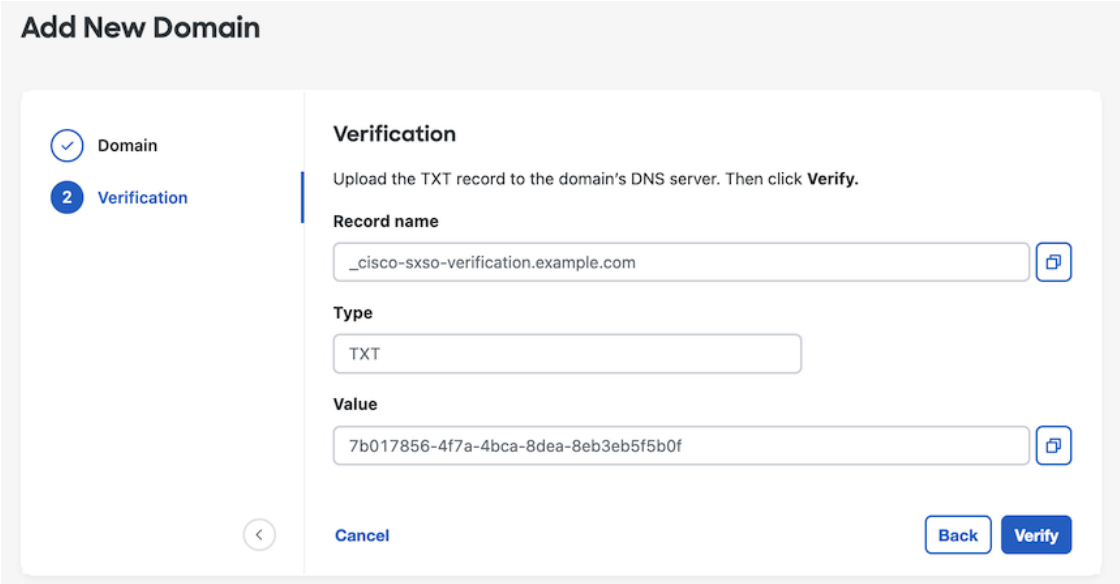
手順

ステップ 1 [Security Provisioning and Administration] ナビゲーションメニューで、[ドメイン（Domains）] をクリックします。

ステップ 2 [ドメイン（Domain）] ページで、 [+ドメインの追加（+ Add domain）] をクリックします。

ステップ 3 [新しいドメインの追加（Add New Domain）] ページで、要求するドメイン名を入力し、[次へ（Next）] をクリックします。

[検証（Verification）]ページには、ドメインレジストラで作成する必要があるテキストレコードの、[レコード名（Record Name）] の下に名前と、[値（Value）] の下に値が表示されます。



ステップ 4 新しいブラウザタブで、ドメイン名レジストラサービスにサインインします。

ステップ 5 指定された**レコード名**と Security Provisioning and Administration から提供された**値**を使用して、新しい TXT レコードを作成します。

ステップ 6 変更を保存し、DNS レコードが反映されるまで待ちます。

ステップ 7 [新しいドメインの追加（Add New Domain）] ページに戻り、[検証（Verify）] をクリックします。

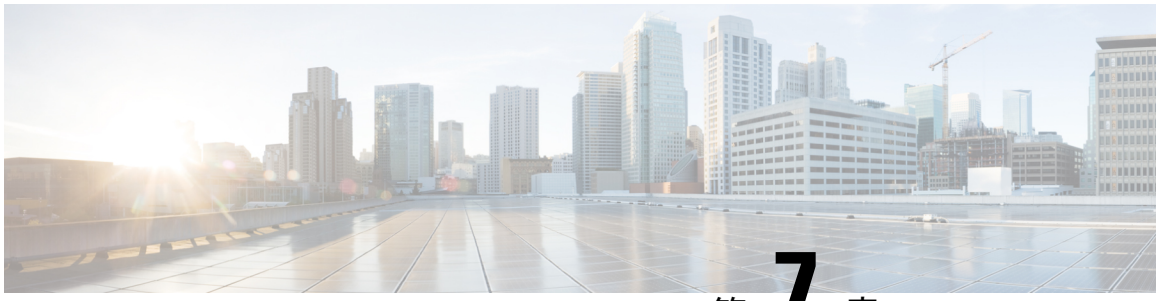
検証に失敗した場合は、次の手順を試してください。

- DNS レコードが反映されるまでしばらく待ちます。
- ドメインレジストラで作成した DNS レコードのタイプ、名前、値が Security Provisioning and Administration で生成された値と一致することを検証します。

次のタスク

電子メールドメインを検証したら、次の操作を実行できます。

- Security Cloud Sign On と ID プロバイダー統合ガイド
- 要求されたドメイン内のユーザーのユーザーパスワードのリセットします。



第 7 章

ID プロバイダー統合ガイド

セキュリティ アサーション マークアップ言語（SAML）を使用してアイデンティティ（ID）プロバイダーを Security Cloud Sign On と統合し、エンタープライズのユーザーに SSO を提供できます。デフォルトでは、Security Cloud Sign On はすべてのユーザーを Duo 多要素認証（MFA）に追加費用なしで登録します。組織ですでに MFA が IdP と統合されている場合、統合中に必要に応じて Duo ベースの MFA を無効にすることができます。

特定の ID サービス プロバイダーと統合する手順については、次のガイドを参照してください。

- Auth0 の Security Cloud Sign On との統合
- Microsoft Entra ID の Security Cloud Sign On との統合
- Duo の Security Cloud Sign On との統合
- Google ID の Security Cloud Sign On との統合
- Okta の Security Cloud Sign On との統合
- Ping ID の Security Cloud Sign On との統合

（注） ID プロバイダーの統合後、ドメイン内のユーザーの認証には、シスコや Microsoft のソーシャルログインなどではなく、統合した ID プロバイダーを使用する必要があります。

前提条件

ID プロバイダーを Security Cloud Sign On と統合するには、次のものが必要です。

- ドメインの要求および検証
- ID プロバイダーの管理ポータルで SAML アプリケーションを作成および構成する機能

SAML 応答の要件

Security Cloud Sign On からの SAML 認証要求への応答として、ID プロバイダーは SAML 応答を送信します。ユーザーが正常に認証された場合、応答には `NameID` 属性とその他のユーザー属性を含む SAML アサーションが含まれます。SAML 応答は、以下で説明する特定の基準を満たす必要があります。

SHA-256 署名付き応答

ID プロバイダーからの応答の SAML アサーションには、次の属性名を含める必要があります。これらの名前は、IdP のユーザープロファイルの対応する属性にマッピングする必要があります。IdP ユーザープロファイル属性名はベンダーによって異なります。

SAML アサーション属性

ID プロバイダーからの応答の SAML アサーションには、次の属性名を含める必要があります。これらの名前は、IdP のユーザープロファイルの対応する属性にマッピングする必要があります。IdP ユーザープロファイル属性名はベンダーによって異なります。

SAML アサーション属性名	ID プロバイダーのユーザー属性
firstName	ユーザーの名。
lastName	ユーザーの姓。
email	ユーザーの電子メール。これは、SAML 応答の **<NameID>** 要素と一致させる必要があります（以下参照）。

<NameID> 要素フォーマット

SAML 応答の `<NameID>` 要素の値は有効な電子メールアドレスにする必要があり、アサーションの `email` 属性の値と一致させる必要があります。`<NameID>` 要素のフォーマット属性を次のいずれかに設定する必要があります。

- `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

SAML アサーションの例

次の XML は、ID プロバイダーから Security Cloud Sign On ACL URL への SAML 応答の例です。**jsmith@example.com** は `<NameID>` 要素であり、また `email` SAML 応答属性です。

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id95383894959750298492624 25" IssueInstant="2023-08-02T01:13:04.861Z"
 Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
    <saml2:Subject>
        <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jsmith@example.com</saml2:NameID>

        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2023-08-02T01:18:05.160Z"
Recipient="https://sso.security.cisco.com/sso/saml2/0oa1rs8y79aeweVg80h8"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2023-08-02T01:08:05.160Z"
NotOnOrAfter="2023-08-02T01:18:05.160Z">
        <saml2:AudienceRestriction>

<saml2:Audience>https://www.okta.com/saml2/service-provider/12345678890</saml2:Audience>

        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2023-08-02T01:13:04.861Z">
        <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>

        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="firstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Joe
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Smith
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jsmith@example.com
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

ステップ1：初期設定

始める前に

まず、Secure Cloud エンタープライズの名前を指定し、無料の Duo 多要素認証（MFA）にユーザーを登録するか、独自の MFA ソリューションを使用するかを決定する必要があります。

すべての統合について、シスコのセキュリティ製品内の機密データを保護するために、セッションタイムアウトを 2 時間以下に設定して MFA を実装することを強く推奨します。

手順

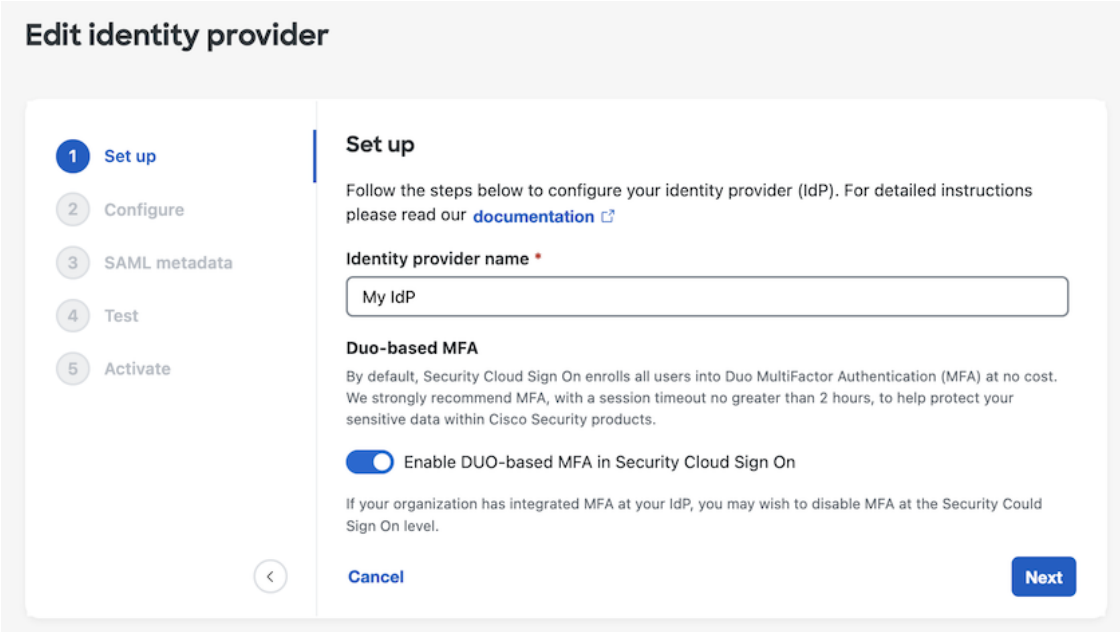
ステップ1 Security Provisioning and Administration メニューで、[IDプロバイダー（Identity Providers）] を選択します。

ステップ2 [+ IDプロバイダーの追加（+ Add Identity Provider）] をクリックします。

（注）
ドメインをまだ要求していない場合は、代わりに [+ドメインの追加（+ Add Domain）] ボタンが表示されます。そのボタンをクリックして、ドメインの要求および検証を開始します。

ステップ3 [セットアップ（Set Up）] ペインで ID プロバイダー名を入力します。

ステップ4 必要であれば、ドメインの要求および検証のユーザーに対して Duo MFA をオプトアウトします。



ステップ5 [次へ（Next）] をクリックして [設定（Configure）] ページに進みます。

ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する

この手順では、Security Provisioning and Administration から提供される SAML メタデータと署名証明書を使用して、ID プロバイダーの SAML アプリケーションを構成します。これには、次の事項が含まれます。

- **シングル サインオンサービス URL**：アサーション コンシューマ サービス（ACS）URL とも呼ばれます。これは、ID プロバイダーがユーザーの認証後に SAML 応答を送信する場所です。
- **エンティティ ID**：オーディエンス URI とも呼ばれます。ID プロバイダーを Security Cloud Sign On で一意に識別するための ID です。
- **署名証明書**：ID プロバイダーが認証要求で Security Cloud Sign On によって送信された署名を検証するために使用する X.509 署名証明書です。

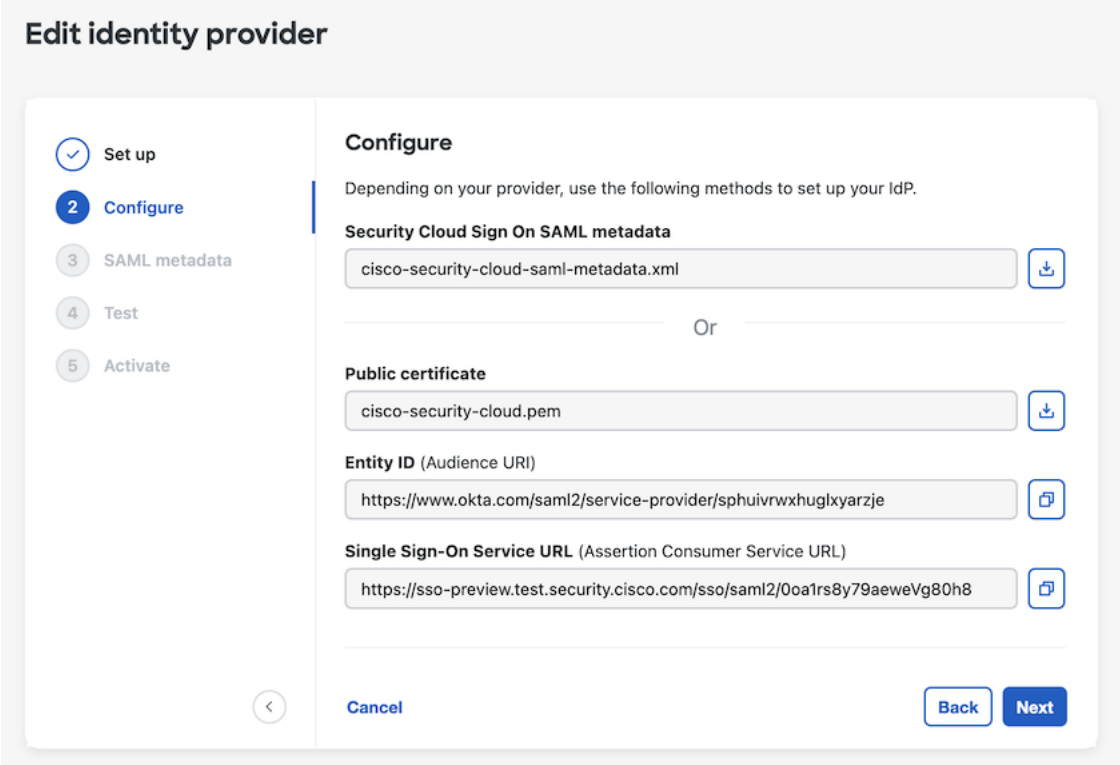
Security Cloud は、ID プロバイダーにアップロードできる単一の SAML メタデータファイルでこの情報を提供し（サポートされている場合）、個々の値としてコピーして貼り付けることができます。市販の ID サービス プロバイダーに固有の手順については、「ID サービスプロバイダーの手順 （67 ページ）」を参照してください。

手順

ステップ 1 ID プロバイダーにより SAML メタデータファイルがサポートされている場合は、それを **[IDプロバイダー（Identity Providers）]** > **[IDプロバイダーの編集（Edit identity provider）]** > **[設定（Configure）]**ページからダウンロードします。サポートされていない場合は、[シングルサインオンサービス（Single Sign-On Service）] と [エンティティID（Entity ID）] の値をコピーし、パブリック証明書をダウンロードします。

ステップ 2 ID プロバイダーで、Security Cloud Sign On と統合する SAML アプリケーションを開きます。

ステップ 3 プロバイダーにより SAML メタデータファイルがサポートされている場合は、それをアップロードします。サポートされていない場合は、必要な Security Cloud Sign On SAML URI をコピーして SAML アプリケーションの設定フィールドに貼り付け、Security Cloud Sign On 公開署名証明書をアップロードします。



ステップ4 前の手順で取得したSecurity Cloud Sign On SAMLメタデータを使用してSAMLアプリケーションを設定します。これには、XMLメタデータファイルをインポートするか、SSOサービスURLとエンティティIDの値を手動で入力し、公開署名証明書をアップロードします。

ステップ5 Security Provisioning and Administrationに戻り、[**次へ（Next）**]をクリックします。

次のタスク

次に、IDプロバイダーのSAMLアプリケーションに対応するメタデータをSecurity Provisioning and Administrationに提供します。

ステップ3：IdPからSecurity CloudにSAMLメタデータを提供する

Security Provisioning and AdministrationのSAMLメタデータを使用してステップ2：IDプロバイダーにSecurity Cloud SAMLメタデータを提供するしたら、次の手順で、対応するメタデータをSAMLアプリケーションからSecurity Provisioning and Administrationに提供します。市販のIDサービスプロバイダーに固有の手順については、「IDサービスプロバイダーの手順（67ページ）」を参照してください。

始める前に

この手順を完了するには、ID プロバイダーの SAML アプリケーションに次のメタデータが必要です。

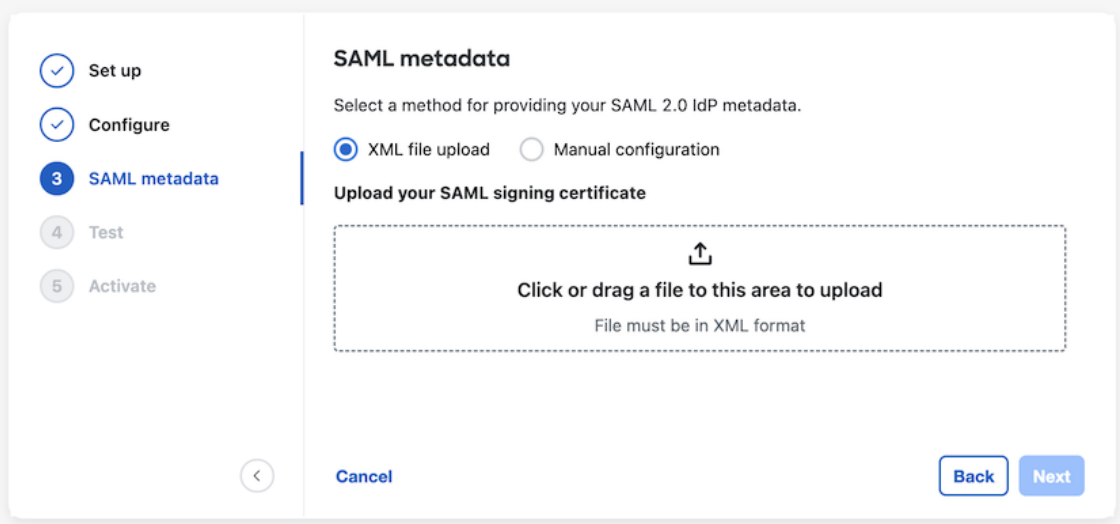
- シングルサインオンサービス URL
- エンティティ ID（オーディエンス URI）
- PEM 形式の署名証明書

ID プロバイダーのデータ提供方法に応じて、上記の情報をすべて含むメタデータ XML ファイルをアップロードするか、個々の SAML URI を手動で入力（コピーして貼り付け）して署名証明書をアップロードできます。市販の ID サービス プロバイダーに固有の手順については、「ID サービスプロバイダーの手順 （67 ページ）」を参照してください。

手順

ステップ 1 Security Provisioning and Administration の **[IDプロバイダー（Identity Providers）] > [IDプロバイダーの編集（Edit identity provider）] > [SAMLメタデータ（SAML metadata）]**ページで、次のいずれかを実行します。

- ID プロバイダーからの XML メタデータファイルがある場合は、[XMLファイルのアップロード（XML file upload）] を選択し、XML ファイルをアップロードします。
- ファイルがない場合は、[手動構成（Manual configuration）] をクリックし、シングルサインオンサービス URL のエンドポイントとエンティティ ID を入力し、ID プロバイダーから提供された公開署名証明書をアップロードします。



ステップ 2 [次へ（Next）] をクリックします。

次のタスク

次に、Security Provisioning and Administration から ID プロバイダーへの SSO を開始して、ステップ 4：SAML 統合のテスト。

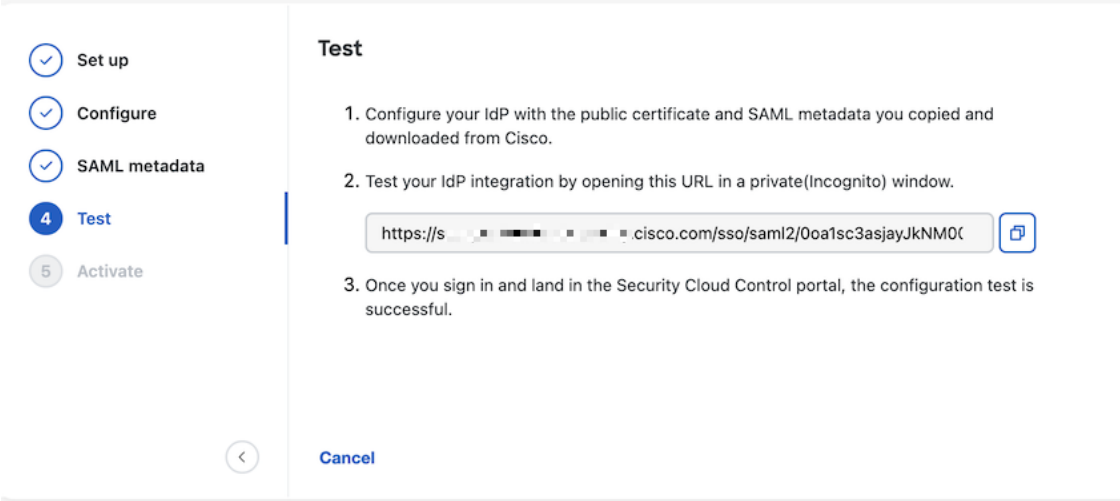
ステップ4：SAML統合のテスト

SAML アプリケーションと Security Cloud Sign On の間で SAML メタデータを交換したら、統合をテストできます。Security Cloud Sign On は、ID プロバイダーの SSO URL に SAML 要求を送信します。ID プロバイダーがユーザーを正常に認証すると、ユーザーは Application Portal にリダイレクトされ、自動的にサインインします。

重要：Security Provisioning and Administration で SAML 統合を作成したときに使用したものとは別の SSO ユーザーアカウントでテストしてください。たとえば、admin@example.com を使用して統合を作成した場合は、別の SSO ユーザー（jsmith@example.com など）でテストします。

手順

ステップ1 Security Provisioning and Administration の **[IDプロバイダー（Identity Providers）]** > **[IDプロバイダーの編集（Edit identity provider）]** > **[テスト（Test）]** ページから、サインイン URL をクリップボードにコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。



ステップ2 ID プロバイダーにサインインします。

ID プロバイダーで認証された後、Application Portal にサインインしている場合、テストは成功です。エラーが表示された場合は、「SAML エラーのトラブルシューティング （66 ページ）」を参照してください。

[次へ（Next）] をクリックして [アクティブ化（Activate）] ステップに進みます。

ステップ 5：統合のアクティブ化

ステップ 4：SAML 統合のテストした後で、アクティブ化できます。統合をアクティブにすると、次のような影響があります。

- 検証済みドメインのユーザーは、統合した ID プロバイダーを使用して認証する**必要があります**。ユーザーがシスコや Microsoft のソーシャル サインオン オプションを使用してサインオンしようとすると、400 エラーが発生します。
- ドメインの要求および検証と一致する電子メールドメインを使用して Security Cloud Sign On にサインインするユーザーは、認証のために ID プロバイダーにリダイレクトされます。
- Duo MFA にオプトインした場合、要求されたドメインのユーザーは MFA 設定を管理できなくなります。

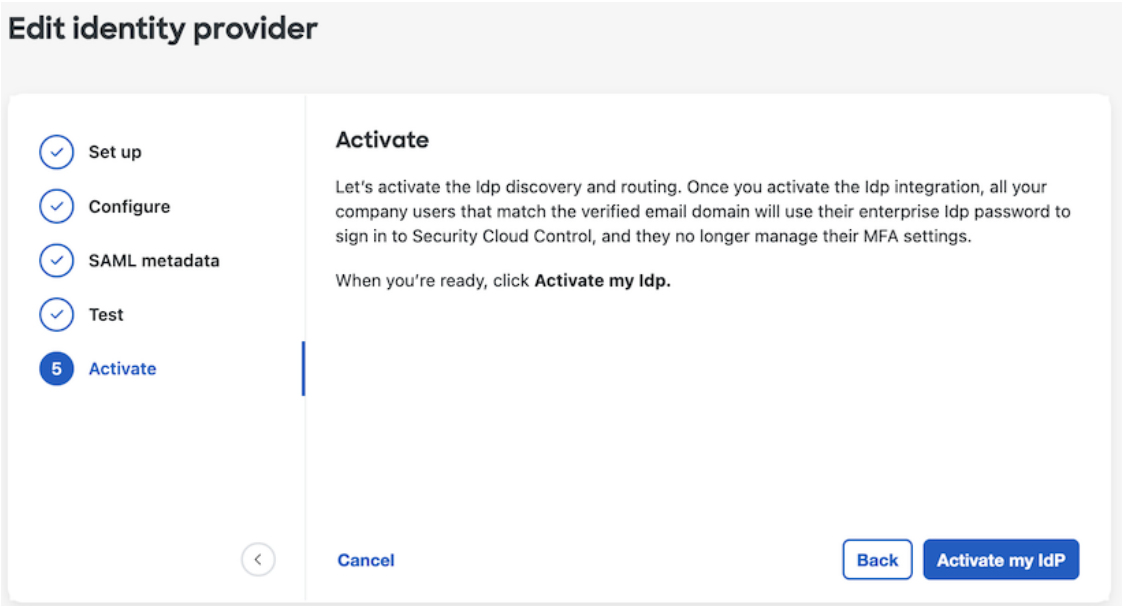
注意 統合をアクティブ化する前に、必ずステップ 4：SAML 統合のテスト。

次の方法で統合をアクティブ化できます。

手順

ステップ 1 Security Provisioning and Administration メニューで、[IDプロバイダー（Identity Providers）] を選択します。

ステップ 2 **[IDプロバイダー（Identity Providers）] > [IDプロバイダーの編集（Edit identity provider）] > [アクティブ化（Activate）]** ページで、[IdPをアクティブ化（Activate my IdP）] をクリックします。



ステップ 3 ダイアログボックスで [アクティブ化（Activate）] をクリックしてアクションを確認します。

SAML エラーのトラブルシューティング

ステップ 4：SAML 統合のテストで HTTP 400 エラーが発生する場合は、次のトラブルシューティング手順を試してください。

ユーザーのサインオン電子メールドメインが要求されたドメインと一致することを確認する

テストに使用しているユーザーアカウントの電子メールドメインがドメインの要求および検証と一致していることを確認してください。
たとえば、`example.com` のような最上位ドメインを申請した場合、ユーザーは `<username>@signon.example.com` ではなく `<username>@example.com` でサインインする必要があります。

ユーザーが ID プロバイダーを使用してサインインしていることを確認する

ユーザーは統合 ID プロバイダーを使用して認証する必要があります。ユーザーがシスコや Microsoft ソーシャル サインイン オプションを使用してサインインするか、Okta から直接サインインしようとすると、HTTP 400 エラーが返されます。

SAML 応答の <NameID> 要素が電子メールアドレスであることを確認する

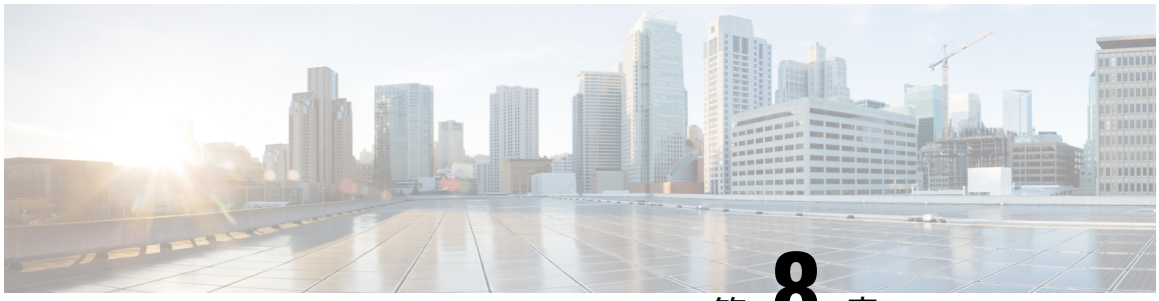
SAML 応答の `<NameId>` 要素の値は電子メールアドレスでなければなりません。電子メールアドレスは、ユーザーの SAML 属性で指定された **email** と一致する必要があります。詳細については、「SAML 応答の要件 （58 ページ）」を参照してください。

SAML 応答に正しい属性要求が含まれていることを確認する

IdP から Security Cloud Sign On への SAML 応答には、必須のユーザー属性である **firstName**、**lastName**、および **email** が含まれます。詳細については、「SAML 応答の要件 （58 ページ）」を参照してください。

IdP からの SAML 応答が SHA-256 で署名されていることを確認する

ID プロバイダーからの SAML 応答は、SHA-256 署名アルゴリズムで署名する必要があります。Security Cloud Sign On は、署名されていないアサーションまたは別のアルゴリズムで署名されたアサーションを拒否します。



第 8 章

ID サービスプロバイダーの手順

このガイドでは、Security Cloud Sign On をさまざまなアイデンティティ（ID）サービスプロバイダーと統合する手順について説明します。

Auth0 の Security Cloud Sign On との統合

このガイドでは、Auth0 SAML Addon を Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド （57 ページ）」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ）」について、Auth0 SAML 統合に固有の詳細を補足します。

手順

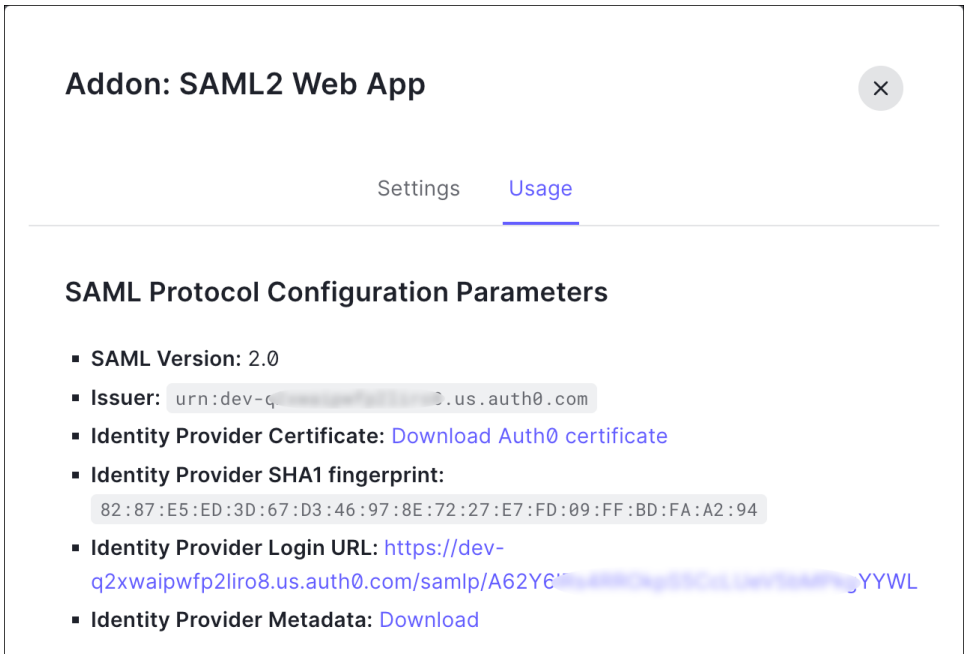
ステップ 1 Auth0 と統合する エンタープライズ で Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定 （60 ページ）」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティ ID（Entity ID）] と [シングルサインオンサービス URL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、管理者としてAuth0組織にサインインします。すぐに戻るので、Security Provisioning and Administration ブラウザタブは開いたままにしておきます。

a) [アプリケーション（Applications）] メニューから [アプリケーション（Applications）] を選択します。
b) [アプリケーションの作成（Create Application）] をクリックします。
c) [名前（Name）] フィールドに「**Secure Cloud Sign On**」または他の名前を入力します。
d) アプリケーションタイプとして [通常のWebアプリケーション（Regular Web Applications）] を選択し、[作成（Create）] をクリックします。
e) [アドオン（Addons）] タブをクリックします。
f) [SAML2 Web App（SAML2 Web App）] トグルをクリックしてアドオンを有効にします。
[SAML2 Webアプリケーションの構成（SAML2 web App configuration）] ダイアログが開きます。

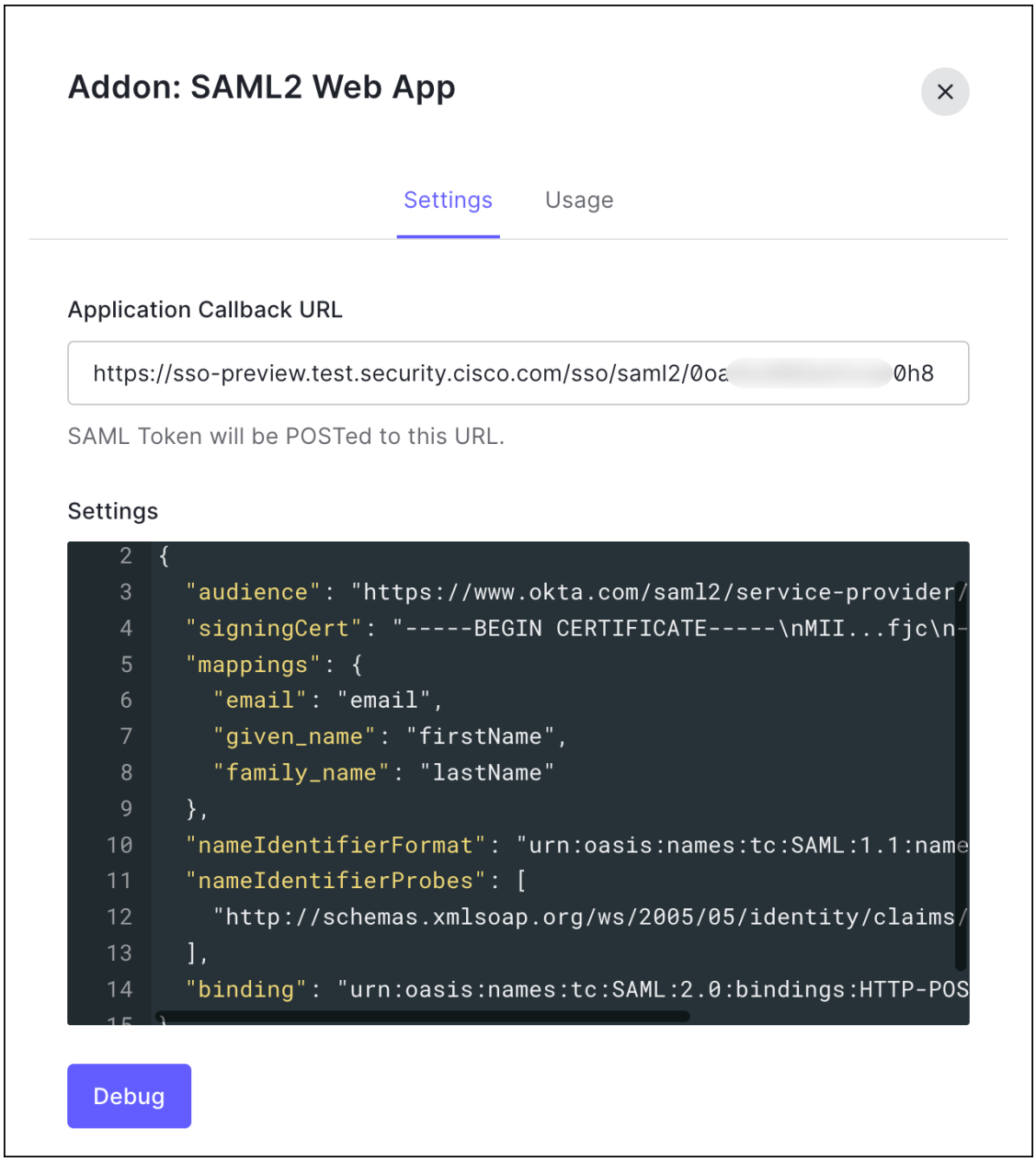


g) [使用（Usage）] タブで、Auth0 の [IDプロバイダー証明書（Identity Provider Certificate）] と [IDプロバイダーのメタデータ（Identity Provider Metadata）] ファイルをダウンロードします。
h) [設定（Settings）] タブをクリックします。
i) [アプリケーションコールバックURL（Application Callback URL）] フィールドに、エンタープライズ設定ウィザードからコピーした [シングルサインオンサービスURL（Single Sign-On Service URL）] の値を入力します。
j) [設定（Settings）] フィールドに次のJSONオブジェクトを入力します。「`audience`」の値は、提供された [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] の値に置き換え、「`signingCert`」は、Security Provisioning and Administration から提供された署名証明書の内容を 1 行のテキストに変換したものに置き換えます。

（注）
Cisco Security Cloud Sign On でログインするには、名と姓を入力する必要があります。Auth0 で使用されるユーザー アイデンティティ ソースによっては、SAML アサーションでユーザーの姓名を使用するために、追加の設定が必要になる場合があります。

次の例は、JSON で given_name と family_name の属性が使用可能で、SAML アサーションで firstName と lastNam にそれぞれマッピングすることを想定しています。

```
{
  "audience": "...",
  "signingCert": "-----BEGIN CERTIFICATE-----\n...-----END CERTIFICATE-----\n",
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
  },
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  ],
  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
}
```



k) [Addon] ダイアログの下部にある [有効化（Enable）] をクリックしてアプリケーションを有効にします。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ） の画面が表示されます。

a) [XMLファイルのアップロード（XML file upload）] オプションを選択します。

b) Auth0 から提供された [IDプロバイダーのメタデータ（Identity Provider Metadata）] ファイルをアップロードします。

次のタスク

次に、「ステップ 4：SAML 統合のテスト （64 ページ）」および「ステップ 5：統合のアクティブ化 （65 ページ）」の手順に従って、統合をテストしてアクティブ化します。

Microsoft Entra ID の Security Cloud Sign On との統合

このガイドでは、Microsoft Entra ID と Security Provisioning and Administration を統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド （57 ページ）」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ）」について、Microsoft Entra ID SAML 統合に固有の詳細を補足します。

手順

ステップ 1 Microsoft Entra ID と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定 （60 ページ）」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティ ID（Entity ID）] と [シングルサインオンサービス URL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、https://portal.azure.com に管理者としてサインインします。すぐに戻るので、Security Provisioning and Administration タブは開いたままにしておきます。

アカウントで複数のテナントにアクセスできる場合は、右上隅でアカウントを選択します。ポータルセッションを必要な Microsoft Entra ID テナントに設定します。

a) [Azure Active Directory] をクリックします。

b) 左側のサイドバーで [エンタープライズアプリケーション（Enterprise Applications）] をクリックします。

c) [+新しいアプリケーション（+ New Application）] をクリックし、[Microsoft Entra SAML Toolkit] を探します。

d) [Microsoft Entra SAML Toolkit] をクリックします。

e) [名前（Name）] フィールドに「**`Security Cloud Sign On`**」またはその他の値を入力し、[作成（Create）] をクリックします。

f) [概要（Overview）] ページで、左側のサイドバーの [管理（Manage）] の下にある [シングルサインオン（Single Sign On）] をクリックします。

g) [シングルサインオン方式の選択（select single sign on method）] で [SAML（SAML）] を選択します。

h) [基本的なSAML構成（Basic SAML Configuration）] パネルで [編集（Edit）] をクリックし、以下を行います。

- [識別子（エンティティID）（Identifier (Entity ID)）] で、[識別子の追加（Add Identifier）] をクリックし、Security Provisioning and Administration から提供された [エンティティID（Entity ID）] の URL を入力します。
- [応答URL（アサーションコンシューマサービスURL）（Reply URL (Assertion Consumer Service URL)）] で、[応答URLの追加（Add Reply URL）] をクリックし、Security Provisioning and Administration からの [シングルサインオンサービスURL（Single Sign-On Service URL）] を入力します。
- [サインオンURL（Sign on URL）] フィールドに「**`https://sign-on.security.cisco.com/`**」と入力します。
- [保存（Save）] をクリックし、[基本的なSAML構成（Basic SAML Configuration）] パネルを閉じます。

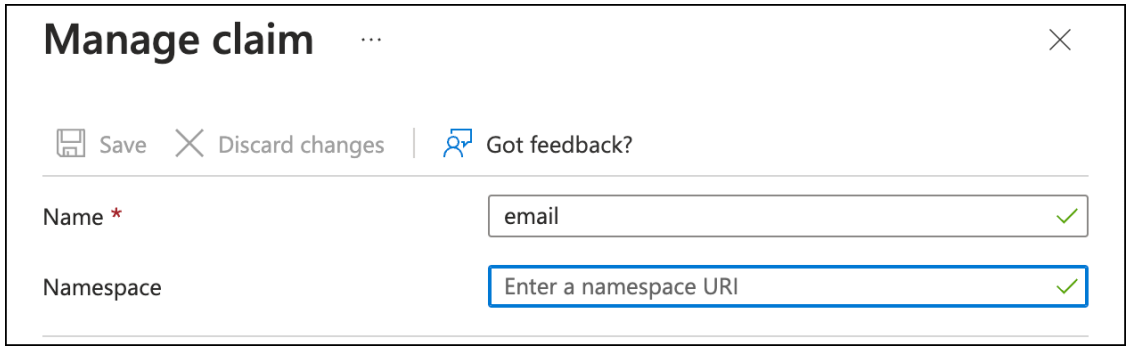
i) [属性と要求（Attributes & Claims）] パネルで、[編集（Edit）] をクリックします。

- [必要な要求（Required claim）] で [一意のユーザー識別子（名前ID）（Unique User Identifier (Name ID)）] 要求をクリックして編集します。
- [ソース属性（Source attribute）] フィールドを `user.userprincipalname` に設定します。ここでは、**user.userprincipalname** の値が有効な電子メールアドレスを表していることを前提としています。それ以外の場合は、[ソース（Source）] を「**user.primaryauthoritativeemail**」に設定します。

j) [追加の要求（Additional Claims）] パネルで [編集（Edit）] をクリックし、Microsoft Entra ID ユーザープロパティと SAML 属性の間の次のマッピングを作成します。

名前	名前空間	ソース属性
`email`	値なし	`user.userprincipalname`
`firstName`	値なし	`user.givenname`
`lastName`	値なし	`user.surname`

次に示すように、要求ごとに [名前空間（Namespace）] フィールドは必ずクリアしてください。



k) [SAML証明書（SAML Certificates）] パネルで、[証明書（Base64）（Certificate (Base64)）] 証明書の [ダウンロード（Download）] をクリックします。

l) この手順で後ほど使用するために、[SAMLによるシングルサインオンのセットアップ（Set up Single Sign-On with SAML）] セクションで [ログインURL（Login URL）] と [Microsoft Entra識別子（Microsoft Entra Identifier）] の値をコピーします。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ） の画面が表示されます。

a) [手動構成（Manual Configuration）] オプションを選択します。

b) [シングルサインオンサービスURL（アサーションコンシューマサービスURL）（Single Sign-on Service URL (Assertion Consumer Service URL)）] フィールドに、Azure から提供された [ログインURL（Login URL）] の値を入力します。

c) [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドに、Microsoft Entra ID によって提供される [Microsoft Entra識別子（Microsoft Entra Identifier）] の値を入力します。

d) Azure で提供された**署名証明書**をアップロードします。

（注）
Azure によって提供される署名証明書ファイルの拡張子は **.cer** です。ただし、Security Provisioning and Administration で証明書を受け入れるには、ファイル拡張子を **.cert** に変更してからアップロードします。

ステップ 4 Security Provisioning and Administration で [次へ（Next）] をクリックします。

次のタスク

「ステップ 4：SAML 統合のテスト （64 ページ）」および「ステップ 5：統合のアクティブ化（65 ページ）」に従って、統合をテストしてアクティブ化します。

Duo の Security Cloud Sign On との統合

このガイドでは、Duo SAML アプリケーションを Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド （57 ページ）」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ）」について、Duo SAML 統合に固有の詳細を補足します。

手順

ステップ 1 Duo と統合する エンタープライズ で Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定 （60 ページ）」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティ ID（Entity ID）] と [シングルサインオンサービス URL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、管理者として Duo 組織にサインインします。すぐに戻るので、Security Provisioning and Administration タブは開いたままにしておきます。

a) 左側のナビゲーションメニューから **[アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）]**をクリックします。

b) 検索バーで、**Cisco Security Cloud Sign On** と検索します。

c) [汎用サービスプロバイダー（Generic Service Provider）] アプリケーションの横にある [保護（Protect）] をクリックし、保護タイプとして [Duoがホストする SSOによる2FA（2FA with SSO hosted by Duo）] を選択します。

汎用 SAML サービスプロバイダーの構成ページが開きます。

d) [メタデータ（Metadata）] セクションを選択します。

e) [エンティティ ID（Entity ID）] の値をコピーし、後で使用するために保存します。

f) [シングルサインオン URL（Single Sign-On URL）] の値をコピーし、後で使用するために保存します。

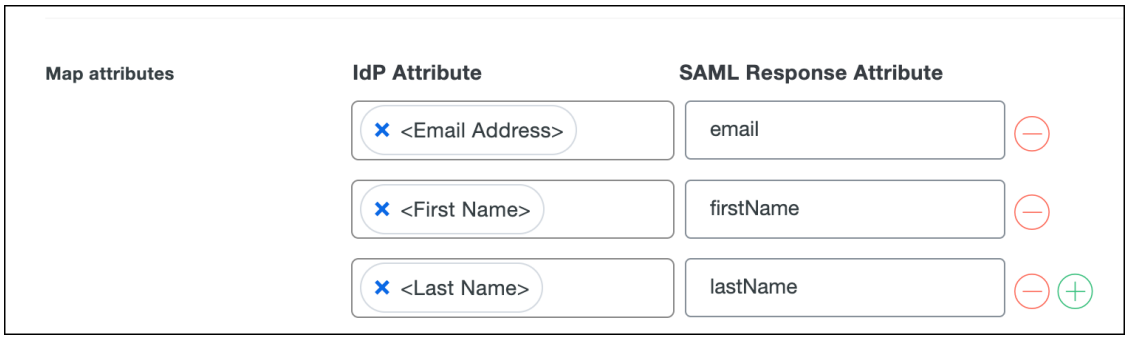
g) 後で使用するため、[ダウンロード（Downloads）] セクションで [証明書のダウンロード（Download certificate）] をクリックします。

h) [SAML応答（SAML Response）] セクションで次の手順を実行します。

- [NameID形式（NameID format）] で [urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified] または [urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress] を選択します。
- [NameID属性（NameID attribute）] で [<Email Address>] を選択します。
- [属性のマッピング（Map Attributes）] セクションで、Duo IdP ユーザー属性と SAML 応答属性の次のマッピングを入力します。

IdP属性（IdP Attribute）	**SAML応答属性（SAML Response Attribute）**
<Email Address>	**email**

IdP属性（IdP Attribute）	SAML応答属性（SAML Response Attribute）
<First Name>	firstName
<Last Name>	lastName



i) [設定（Settings）] の [名前（Name）] フィールドに「**Security Cloud Sign On**」または他の値を入力します。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ） の画面が表示されます。

a) [手動構成（Manual Configuration）] オプションを選択します。
b) [シングルサインオンサービスURL（アサーションコンシューマサービスURL）（Single Sign-on Service URL (Assertion Consumer Service URL)）] フィールドに、Duo から提供された [シングルサインオンURL（Single Sign-On URL）] の値を入力します。
c) [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドに、Duo から提供された [エンティティID（Entity ID）] の値を入力します。
d) Duo からダウンロードした**署名証明書**をアップロードします。

次のタスク

次に、「ステップ 4：SAML 統合のテスト （64 ページ）」および「ステップ 5：統合のアクティブ化 （65 ページ）」の手順に従って、統合をテストしてアクティブ化します。

Google ID の Security Cloud Sign On との統合

このガイドでは、Google ID SAML アプリケーションを Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド （57 ページ）」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」および「ステップ 3：IdP から Security

Cloud に SAML メタデータを提供する （62 ページ）」について、Google ID 統合に固有の詳細を補足します。

手順

ステップ 1 Google と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定 （60 ページ）」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティ ID（Entity ID）] と [シングルサインオンサービスURL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、スーパー管理者権限を持つアカウントを使用して Google 管理コンソールにサインインします。Security Provisioning and Administration タブは開いたままにします。

a) 管理コンソールで、メニュー ☰ > [アプリ（Apps）] > [ウェブアプリとモバイルアプリ（Web and mobile apps）] に移動します。

b) [アプリを追加（Add App）] > [カスタムSAMLアプリの追加（Add custom SAML app）] をクリックします。

c) [アプリの詳細（App Details）] で以下を行います。

- アプリケーション名に「**`Secure Cloud Sign On`**」または他の値を入力します。
- 必要に応じて、アプリケーションに関連付けるアイコンをアップロードします。

d) [続行（Continue）] をクリックして、[Google ID プロバイダー（Google Identity Provider）] の詳細ページに移動します。

e) [メタデータのダウンロード（Download Metadata）] をクリックして、後で使用するために Google SAML メタデータファイルをダウンロードします。

f) [続行（Continue）] をクリックして、[サービスプロバイダーの詳細（Service provider details）] ページに移動します。

g) [ACS URL（ACS URL）] フィールドに、Security Provisioning and Administration から提供された [シングルサインオンサービスURL（Single Sign-On Service URL）] を入力します。

h) [エンティティ ID（Entity ID）] フィールドに、Security Provisioning and Administration から提供された [エンティティ ID（Entity ID）] の URL を入力します。

i) [署名付き応答（Signed Response）] オプションをオンにします。

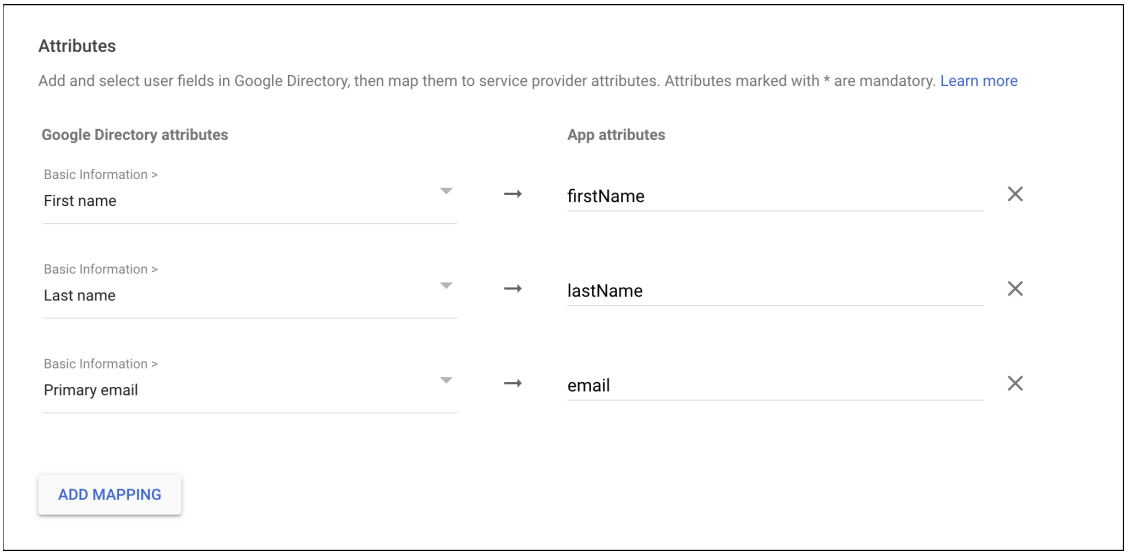
j) [名前IDの形式（Name ID Format）] で [UNSPECIFIED（UNSPECIFIED）] または [EMAIL（EMAIL）] を選択します。

k) [名前ID（Name ID）] で [基本情報 > 主要電子メール（Basic Information > Primary email）] を選択します。

l) [続行（Continue）] をクリックして、[属性マッピング（Attribute mapping）] ページに進みます。

m) Google ディレクトリ属性とアプリケーション属性との次のマッピングを追加します。

Googleディレクトリの属性（Google Directory attributes）	アプリの属性（App attributes）
名（First name）	firstName
姓（Last name）	lastName
Primary email	email



n) [終了（Finish）] をクリックします。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ） の画面が表示されます。

a) [XMLファイルのアップロード（XML file upload）] オプションを選択します。

b) 以前に Google 社からダウンロードした SAML メタデータファイルをアップロードします。

c) [次へ（Next）] をクリックして [テスト（Testing）] ページに進みます。

次のタスク

次に、「ステップ 4：SAML 統合のテスト （64 ページ）」および「ステップ 5：統合のアクティブ化 （65 ページ）」の手順に従って、統合をテストしてアクティブ化します。

Okta の Security Cloud Sign On との統合

このガイドでは、Okta SAML アプリケーションを Security Provisioning and Administration と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド （57 ページ）」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ）」について、Okta SAML 統合に固有の詳細を補足します。

手順

ステップ 1 Okta と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定 （60 ページ）」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティ ID（Entity ID）] と [シングルサインオンサービス URL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、管理者として Okta 組織にサインインします。すぐに戻るので、Security Provisioning and Administration タブは開いたままにしておきます。

a) [アプリケーション（Applications）] メニューから [アプリケーション（Applications）] を選択します。

b) [アプリケーション統合の作成（Create App Integration）] をクリックします。

c) [SAML 2.0（SAML 2.0）] を選択し、[次へ（Next）] をクリックします。

d) [全般設定（General Settings）] タブで、統合の名前（例：**Security Cloud Sign On**）を入力し、必要に応じてロゴをアップロードします。

e) [次へ（Next）] をクリックして [SAMLの構成（Configure SAML）] ページに進みます。

f) [シングルサインオン URL（Single sign-on URL）] フィールドに、Security Provisioning and Administration から提供された [シングルサインオンサービス URL（Single sign-on Service URL）] を入力します。

g) [オーディエンス URI（Audience URI）] フィールドに、Security Provisioning and Administration から提供された [エンティティ ID（Entity ID）] を入力します。

h) [名前IDの形式（Name ID Format）] で [指定なし（Unspecified）] または [電子メールアドレス（EmailAddress）] を選択します。

i) [アプリケーションユーザー名（Application username）] で [Oktaユーザー名（Okta username）] を選択します。

j) [属性ステートメント（オプション）（Attribute Statements (optional)）] セクションで、次の名前 SAML 属性のマッピングを Okta ユーザープロファイルに追加します。

名前（Name）（SAML アサーション）	値（Value）（Okta プロファイル）
email	user.email
firstName	user.firstName
lastName	user.lastName

k) [Show Advanced Settings] をクリックします。

l) [次へ（Next）] をクリックします。

m) [署名証明書（Signature Certificate）] で、[ファイルの参照（Browse files...）] をクリックし、以前に Security Provisioning and Administration からダウンロードした公開署名証明書をアップロードします。

（注）
応答とアサーションは、RSA-SHA256 アルゴリズムで署名する必要があります。

n) [サインオン（Sign On）]、[設定（Settings）]、[サインオン方法（Sign on method）] の順に選択し、[詳細の表示（Show details）] をクリックします。

o) [次へ（Next）] をクリックして Okta にフィードバックを送信し、[完了（Finish）] をクリックします。

p) [サインオンURL（Sign on URL）] と [発行者（Issuer）] の値をコピーし、**署名証明書**をダウンロードして Security Provisioning and Administrationに提供します。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ） の画面が表示されます。

a) [手動構成（Manual Configuration）] オプションを選択します。

b) [シングルサインオンサービスURL（アサーションコンシューマサービスURL）（Single Sign-on Service URL (Assertion Consumer Service URL)）] フィールドに、Okta から提供された [サインオンURL（Sign on URL）] の値を入力します。

c) [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドに、Okta から提供された [発行者（Issuer）] の値を入力します。

d) Okta から提供された**署名証明書**をアップロードします。

次のタスク

次に、「ステップ 4：SAML 統合のテスト （64 ページ）」および「ステップ 5：統合のアクティブ化 （65 ページ）」の手順に従って、統合をテストしてアクティブ化します。

Ping ID の Security Cloud Sign On との統合

このガイドでは、Ping SAML アプリケーションを Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド （57 ページ）」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ）」について、Ping 統合に固有の詳細を補足します。

手順

ステップ 1 Ping と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定 （60 ページ）」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する （61 ページ）」で、後で使用するために **Security Cloud Sign On SAML メタデータ**ファイルをダウンロードします。

ステップ 2 新しいブラウザタブで、Ping 管理コンソールにサインインします。Security Provisioning and Administration ブラウザタブを開いたままにします。

a) [接続（Connections）] > [アプリケーション（Applications）] に移動します。

b) [+] ボタンをクリックして [アプリケーションの追加（Add Application）] ダイアログを開きます。

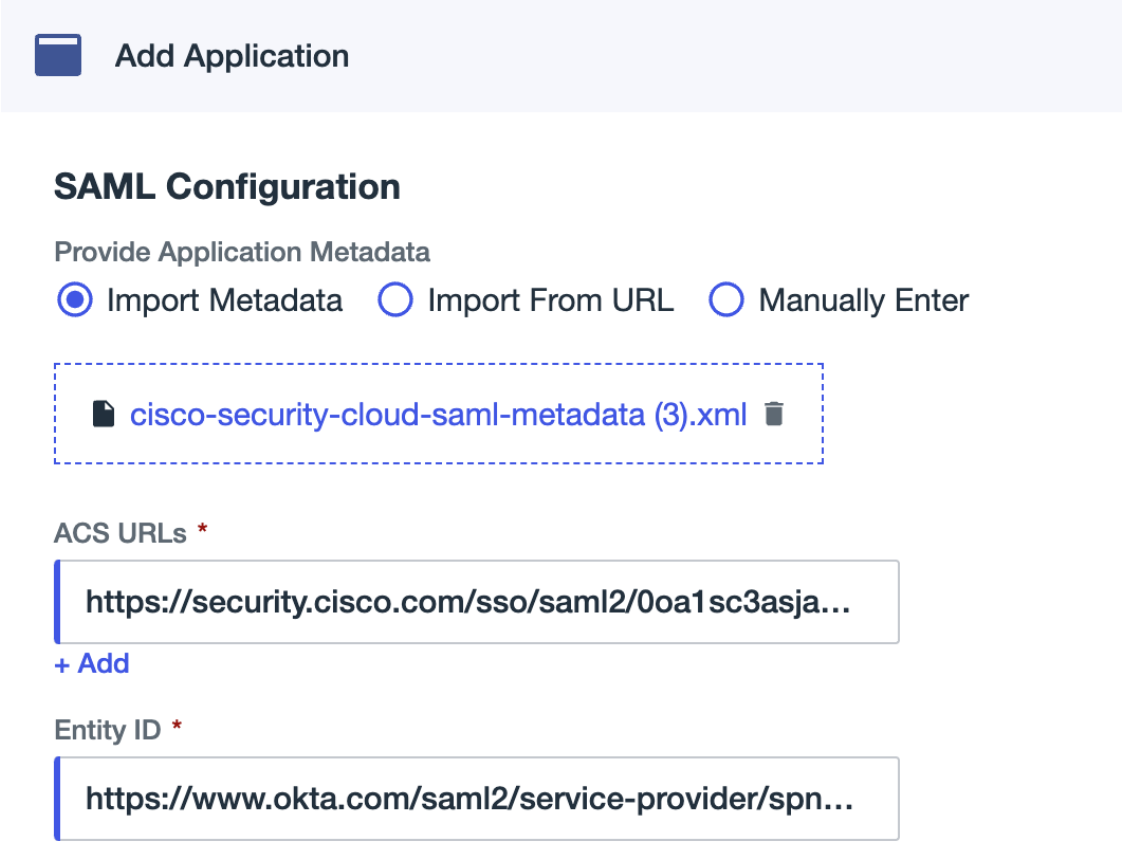
c) [アプリケーション名（Application Name）] フィールドに「**`Secure Cloud Sign On`**」または他の名前を入力します。

d) 必要に応じて、説明を追加し、アイコンをアップロードします。

e) [アプリケーションの種類（Application Type）] で [SAMLアプリケーション（SAML application）] を選択し、[構成（Configure）] をクリックします。

f) [SAML構成（SAML Configuration）] ダイアログで、[メタデータのインポート（Import Metadata）] オプションを選択し、[ファイルの選択（Select a file）] をクリックします。

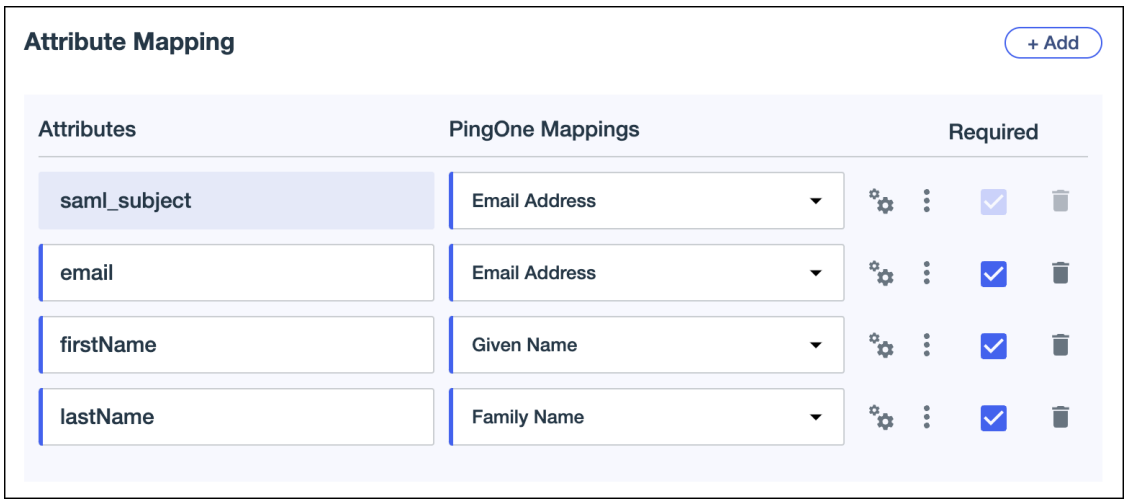
g) Security Provisioning and Administration からダウンロードした **Security Cloud Sign On SAML メタデータ**ファイルを見つけます。



h) [保存（Save）] をクリックします。
i) [設定（Configuration）] タブをクリックします。
j) [メタデータのダウンロード（Download Metadata）] をクリックして、Security Provisioning and Administration に提供する SAML メタデータファイルをダウンロードします。
k) [属性のマッピング（Attribute Mappings）] タブをクリックします。
l) [編集（Edit）]（鉛筆アイコン）をクリックします。
m) 必須の [saml_subject（saml_subject）] 属性について、[電子メールアドレス（Email Address）] を選択します。
n) [+追加（+Add）] をクリックし、SAML 属性と PingOne ユーザー ID 属性の次のマッピングを追加し、それぞれのマッピングで [必須（Required）] オプションを有効にします。

属性	PingOne マッピング（PingOne Mappings）
firstName	電子メール アドレス（Email Address）
lastName	Given Name
email	Family Name

[属性マッピング（Attribute Mapping）] パネルは次のようになります。



o) [保存（Save）] をクリックしてマッピングを保存します。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する （62 ページ） の画面が表示されます。

a) [XMLファイルのアップロード（XML file upload）] オプションを選択します。

b) 以前に Ping からダウンロードした SAML メタデータファイルをアップロードします。

c) [次へ（Next）] をクリックして [テスト（Testing）] ページに進みます。

次のタスク

次に、「ステップ 4：SAML 統合のテスト （64 ページ）」および「ステップ 5：統合のアクティブ化 （65 ページ）」の手順に従って、統合をテストしてアクティブ化します。

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。