テナントとユーザーの管理

Security Cloud Control テナントの管理

Security Cloud Control では、テナント、ユーザー、および通知設定の特定の要素をカスタマイズできます。カスタマイズ設定で使用できる次の設定を確認してください。

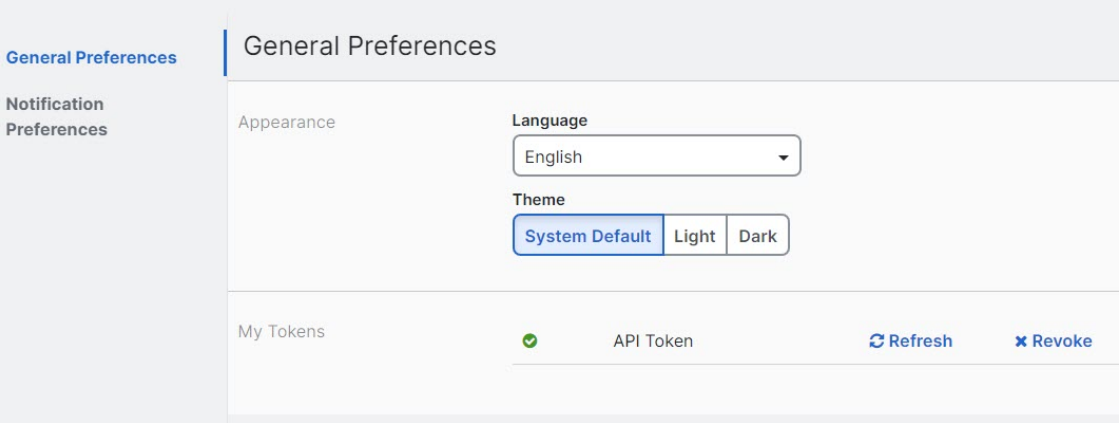
ユーザー設定の指定

一般的な Security Cloud Control 設定に関する次のトピックを参照してください。

- 一般設定 （1 ページ）
- ユーザー通知の基本設定

一般設定

Security Cloud Control UI で表示する言語とテーマを選択します。この選択は、この変更を行うユーザーにのみ影響します。



Security Cloud Control Web インターフェイス表示の変更

Web インターフェイスの表示方法を変更できます。

手順

ステップ 1 ユーザー名の下にあるドロップダウンリストから、[設定（Preferences）] を選択します。

ステップ 2 [一般設定（General Preferences）] エリアで、[テーマ（Theme）] を選択します。

- **低**
- **ダーク**

ユーザー通知の基本設定

Security Cloud Control は、テナントにリンクされているデバイスで特定のイベントが発生するたびに通知を生成します。これには、デバイスによって実行されたアクション、デバイス証明書の期限切れが近づいていることと期限が切れたこと、またはレポート生成タスクの開始、完了、失敗が含まれます。デフォルトでは、これらの通知は有効になっており、ロールに関係なく、テナントに関連付けられているすべてのユーザーに表示されます。個人の通知設定をカスタマイズして、関心のあるアラートだけを表示することができます。これらの設定は各人のものであり、テナントに接続されている他のユーザーには影響しません。

（注） 以下にリストされている通知に加えられた変更は、リアルタイムで自動的に更新され、展開を必要としません。

デバイスワークフローのアラートの送信

- [展開（Deployments）]：このアクションは、SSH またはIOSデバイスの統合インスタンスを含みません。
- [バックアップ（Backups）]：このアクションは FDM-managed デバイスにのみ適用されます。
- [アップグレード（Upgrades）]：このアクションは、ASA および FDM-managed デバイスにのみ適用されます。
- [クラウドへのFirewall Threat Defenseの移行（Migrate to Cloud）]：このアクションは、Firewall Threat Defense の変更時に適用可能です。

  デバイスマネージャを Firewall Management Center から Security Cloud Control に変更すると適用されます。

デバイスイベントのアラートの送信

- [オフラインになる（Went offline）]：このアクションは、テナントに関連付けられているすべてのデバイスに適用されます。
- [オンラインに戻る（Back online）]：このアクションは、テナントに関連付けられているすべてのデバイスに適用されます。
- [競合検出（Conflict detected）]：このアクションは、テナントに関連付けられているすべてのデバイスに適用されます。
- [HA状態の変更（HA state changed）]：このアクションは、HA またはフェールオーバーペア内のデバイス、現在の状態、および変更前の状態を示します。このアクションは、テナントに関連付けられたすべての HA およびフェールオーバー設定に適用されます。
- [サイト間セッションの切断（Site-to-Site session disconnected）]：このアクションは、テナントで設定されているすべてのサイト間 VPN の設定に適用されます。

イベント検索レポート生成のアラートの送信

- [レポート生成開始（Report generation started）]：レポート生成タスクが開始されたときに通知を受け取ります。これは、即時検索レポートとスケジュール済み検索レポートの両方に適用されます。
- [レポート生成完了（Report generation completed）]：レポート生成タスクが終了したときに通知を受け取ります。これは、即時検索レポートとスケジュール済み検索レポートの両方に適用されます。
- [レポート生成失敗（Report generation failed）]：レポート生成タスクが失敗したときに通知を受け取ります。これは、即時検索レポートとスケジュール済み検索レポートの両方に適用されます。パラメータまたはクエリを確認して、再試行してください。

通知のオプトアウトの基本設定

デフォルトでは、すべてのイベントが有効になっており、通知が生成されます。上記のイベントによって生成された通知をオプトアウトするには、通知タイプを手動で**オフ**にする必要があります。変更を確定するには、[保存（Save）] をクリックする必要があります。

電子メールの通知

上記のアラートのいずれかを受信するには、[Email Notification] トグルを有効にします。電子メールで受信するアラートをオンにして、[保存（Save）] ボタンをクリックします。デフォルトでは、[上記のSecurity Cloud Control通知設定を使用する（Use CDO notification settings）] がオンになっています。つまり、このページで説明した「アラートの送信」セクションでオンにしたものと同じ通知およびイベントのすべてに対して、電子メールアラートを受信します。

上記のイベントまたはアラートの**一部**のみを電子メールに転送する場合は、[上記のSecurity Cloud Control通知設定を使用する（Use CDO notification settings above）] をオフにします。このアクションにより、使用可能なアラートを変更およびパーソナライズするための追加の場所が生成されます。これにより、冗長性を削減できる場合があります。

Security Cloud Control 通知の表示

通知アイコン  をクリックして、テナントで発生した最新のアラート、またはテナントにオンボード済みのデバイスに影響を及ぼすアラートを表示します。[通知設定（Notification Settings）] ページでの選択は、Security Cloud Control に表示される通知のタイプに影響します。詳細については、このまま読み進めてください。

このドロップダウンページは、[概要（Overview）]、[すべて（All）]、および [非表示（Dismissed）] の 3 つのタブにグループ化されています。

[概要（Overview）] タブ

[Overview] タブには、登録しているアラートとイベントのうち、最新のものと優先順位の高いものの組み合わせが表示されます。優先順位が高いイベントは次のとおりです。

- 展開に失敗しました
- バックアップに失敗しました
- アップグレードに失敗しました
- FTD から cdFMC への移行に失敗しました
- デバイスがオフラインになりました
- デバイスの HA 状態が変更されました
- デバイス証明書の有効期限が近づいています

受信するアラートを設定するには、[通知（Notifications）] ウィンドウの [通知設定（Notification Settings）] をクリックするか、**[UserID]** > [ユーザー設定（User Preferences）] ページを選択します。ダッシュボードの右上隅にある [ユーザー ID（User ID）] ボタンをクリックします。

[すべて（All）] タブ

[All] タブには、優先順位のランク付けに関係なく、電子メールサブスクリプション通知や優先順位の高いあらゆる項目を含むすべての通知が表示されます。

[非表示（Dismissed）] タブ

[非表示（Dismissed）] タブには、非表示にした通知が表示されます。個々の通知を非表示にするには、通知の [x] をクリックします。

ドロップダウンメニューから通知を [非表示にする（Dismiss）] を選択すると、その通知は [概要（Overview）] タブと [すべて（All）] タブの**両方**で非表示になります。非表示にした通知は 30 日間 [非表示（Dismiss）] タブに残り、その後 Security Cloud Control から削除されます。

通知の検索

通知ドロップダウンウィンドウの表示中は、上記のいずれのタブでも、ドロップダウンの上部にある検索バーを使用して、キーワードまたはアラートをクエリできます。

通知設定の表示

[Notification Preferences] ページで個人設定を表示します。このページでは、次の「**Security Cloud Control で通知**」アラートを設定し、いずれかのアラートを受信できる電子メール通知を有効にできます。「通知設定」を参照してください。

全般設定

[General Settings] は、 管理対象組織内の複数の管理対象デバイスおよびユーザーに影響する、管理対象組織全体の設定をカスタマイズして管理するために使用されます。

（注） 管理対象組織に対して有効になっていない機能のトグルボタンは表示されません。

変更リクエストのトラッキングの有効化

変更要求トラッキングの有効化は、テナントのすべてのユーザーに影響を及ぼします。変更リクエストのトラッキングを有効にするには、次の作業を行います。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 **[変更リクエストのトラッキング（Change Request Tracking）]** トグルボタンを有効にします。

確認が完了すると、インターフェイスの左下隅と、[変更ログ（Change Log）] の [変更要求（Change Request）] ドロップダウンメニューに、[変更要求（Change Request）] ツールバーが表示されます。

デバイスの変更を自動承認するオプションを有効にします

デバイスの変更の自動承認を有効にすると、Security Cloud Control はデバイスで直接行われた変更を自動的に承認できます。このオプションを無効のままにするか、後で無効にする場合は、変更を承認する前に各デバイスの競合を確認する必要があります。

デバイスの変更の自動承認を有効にするには、次の手順を実行します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 **[Enable the option to auto-accept device changes]** トグルボタンをオンにします。

デフォルトの競合検出間隔

この間隔で、Security Cloud Control がオンボーディングされたデバイスの変更をポーリングする頻度が決まります。選択は、このテナントで管理されているすべてのデバイスに適用されます。このオプションはいつでも変更できます。

（注） この選択は、1 つまたは複数のデバイスを選択した後、[セキュリティデバイス（Security Devices）] ページから利用できる [競合検出（Conflict Detection）] オプションを介してオーバーライドできます。

このオプションを設定し、競合検出の新しい間隔を選択するには、次の手順に従います。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 [Default Conflict Detection Interval] のドロップダウンメニューをクリックし、時間の値を選択します。

自動展開をスケジュールするオプションを有効化

自動展開をスケジュールするオプションを有効にすると、都合のよい日時に将来の展開をスケジュールできます。このオプションを有効にすると、単一の自動展開をスケジュールしたり、定期的な自動展開を設定したりできます。自動展開をスケジュールするには、「自動展開のスケジュール」を参照してください。

デバイスの Security Cloud Control で行われた変更は、  に保留中の変更がある場合、デバイスに自動的に展開されません。デバイスが [競合検出（Conflict Detected）] または [未同期（Not Synced）] など、[同期（Synced）] 状態でない場合、スケジュールされた展開は実行されません。[ジョブ（Jobs）] ページには、スケジュールされた展開が失敗したインスタンスが一覧表示されます。

[Enable the Option to Schedule Automatic Deployments] をオフにすると、スケジュールされたすべての展開が削除されます。

重要 Security Cloud Control を使用して、スケジュールされた展開をデバイスに対して複数作成する場合、新しい展開によって既存の展開が上書きされます。API を使用してデバイスのスケジュールされた展開を複数作成する場合は、新しい展開をスケジュールする前に、既存の展開を**削除する必要**があります。

自動展開をスケジュールするオプションを有効にするには、次の手順を実行します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 **[Enable the option to schedule automatic deployments]** トグルボタンをオンにして、有効にします。

Web 分析

Web 分析により、ページのヒット数に基づく匿名の製品使用情報がシスコに提供されます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。このデータは、Cisco が機能の使用状況パターンを確認し、製品を改善する際に役立ちます。すべての使用状況データは匿名で、センシティブデータは送信されません。

Web 分析はデフォルトで有効になっています。Web 分析を無効化、または今後再度有効化するには、次の手順を実行します：

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 **[Web Analytics]** トグルボタンをオンにして有効にします。

Talosとのイベントデータ共有の有効化

Ciscoの脅威インテリジェンス組織であるTalosと、デバイスからの悪意のあるイベントデータを共有します。イベントデータを共有することで、Talos の脅威インテリジェンス機能が向上し、ネットワークにターゲットを絞ったセキュリティインサイトを提供して、新たな脅威に対する保護を強化できます。

Talos の詳細については、Cisco Talos の製品ページを参照してください。

[Enable event data sharing with Talos] トグルボタンをオンにしても、Cloud-Delivered Firewall Management Center の **[Talos Threat Hunting Telemetry]** 機能は自動的にアクティブになりません。この機能で最適な結果を得るには、Cloud-Delivered Firewall Management Center で **Talos脅威ハンティングテレメトリ**も有効にします。詳細については、「侵入ポリシーの設定」を参照してください。

Talos とのイベントデータの共有は、デフォルトで有効になっています。オプトアウトするには、次の手順を実行します。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 **[Enable event data sharing with Talos]** トグルボタンをオフにして、設定を無効化します。

（注）
イベントデータを共有することで、Talos はネットワークに関連するセキュリティインサイトを提供できます。この設定を無効にすると、Talosの機能を最大限に使用する機能が制限され、進化する脅威に対するネットワークの防御に影響を与える可能性があります。

FDMのデフォルトの定期バックアップスケジュール

デバイス間でバックアップスケジュールの一貫性を保つために、この設定を使用して、デフォルトバックアップスケジュールを設定できます。特定のデバイスのバックアップをスケジュールするときは、デフォルト設定を使用することも、変更することもできます。デフォルトの定期バックアップスケジュールを変更しても、既存のスケジュールバックアップとその定期バックアップの設定は同じままです。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 **Administration** > **General Settings** を選択します。

ステップ 3 [Tenant Settings] エリアにある [Default Recurring Backup Schedule] セクションを見つけ、[Frequency] フィールドで、日次、週次、または月次のバックアップを選択します。

ステップ 4 バックアップの日時を入力します。協定世界時（UTC）で 24 時間形式を使用して時刻を入力します。たとえば、22：00（10：00 PM UTC）などです。

ステップ 5 毎週バックアップする場合は、バックアップする曜日を選択します。毎月バックアップする場合は、**[Days of Month]** フィールドを選択し、バックアップを実行する日数を追加します。31 日未満の月に「31 日」と入力した場合、その月のバックアップは実行されません。バックアップスケジュールの名前と説明を入力します。

ステップ 6 [Save] をクリックします。

テナントの詳細

テナントの詳細は、Cisco Technical Assistance Center（TAC）に連絡する必要があるときに役立ちます。コピーアイコンをクリックすると、これらのテナントの詳細をコピーできます。

- **テナント ID**：テナント ID によってテナントが識別されます。
- **企業 ID**： 企業 ID は、企業を識別します。
- **Cisco Security Services Exchange テナントID**：Cisco Security Services Exchange テナントID は、Cisco Secure Services Exchange 環境内のテナントを一意に識別します。これにより、Cisco プラットフォーム間でのセキュリティサービスの統合と管理が容易になります。
- **テナント名**：テナント名は、テナントも識別します。テナント名は組織名ではないことに注意してください。

テナント名

テナント名は、テナントも識別します。テナント名は組織名ではないことに注意してください。この情報は、Cisco Technical Assistance Center（TAC）に連絡する必要があるときに役立ちます。

Security Cloud Control Platform Navigator

Platform Navigator は、Security Cloud Control の右上隅に表示される 9 つのブロック（  ）で、アプリケーションのクロスランチャです。Cisco のこれらのネットワーキングおよびセキュリティアプリケーションを簡単にクロス起動できます。

ネットワーキング アプリケーション

- **Cisco Catalyst**：Cisco Catalyst 製品は、さまざまなネットワークスイッチ、ワイヤレスコントローラ、ワイヤレスアクセスポイント、およびエッジプラットフォームとルータを含み、耐久性が高く堅牢なネットワーキング環境を必要とするエンタープライズクラスのビジネスニーズをサポートします。

- **Cisco Intersight**：Cisco Intersight はクラウド運用プラットフォームであり、先進的なインフラストラクチャのモジュラ型機能、ワークロードの最適化、およびKubernetesサービスなどのオプションで構成されます。Cisco Intersight インフラストラクチャ サービスには、物理および仮想インフラストラクチャの展開、モニタリング、管理、サポートが含まれます。Cisco Unified Computing System（Cisco UCS）、Cisco HyperFlex ハイパーコンバージドインフラストラクチャ（HCI）、およびその他 Intersight に接続されたサードパーティ製のターゲットをサポートします。

- **IoT Operations Dashboard**：Cisco IoT Operations Dashboard は、クラウドベースの IoT サービスプラットフォームであり、オペレーションズチームが産業用ネットワークデバイスおよび接続された大規模な産業資産に安全に接続し、接続を維持し、インサイトを得られるようにします。接続されているすべての産業資産が 1 ヵ所にまとめて表示されるため、業務チームは運用の合理化と事業継続に役立つ有益なインサイトを引き出すことができます。

- **Cisco Meraki**：Cisco Meraki は、Cisco Meraki デバイスの中央管理プラットフォームを提供する、IT および IoT クラウド管理型プラットフォームです。

- **Cisco Spaces**：Cisco Spaces はクラウドベースのロケーション サービス プラットフォームであり、組織は物理スペース内における人や物の移動に関するインサイトを得られます。こうしたインサイトをもとに、有益で関連性の高い、コンテキストに応じたエンゲージメントを提供できます。組織は、人の移動を把握するだけでなく、資産の場所、移動、使用状況をモニタリングすることで、業務効率を向上させることができます。

- **Cisco ThousandEyes**：Cisco ThousandEyes は、Web アプリケーション、サービス、およびネットワークの可用性とパフォーマンスのモニタリングと測定をサポートするクラウドサービススイートです。任意のユーザーに対し、あらゆるネットワーク上のあらゆるアプリケーションがエンドツーエンドで可視化されるため、企業は問題の発生源を迅速に特定し、迅速に解決し、パフォーマンスを効果的に管理できます。

- **Cisco Workflows**：Cisco Workflows は、大規模な Cisco Networking Cloud ビジョンの一部であるクラウドホスト型自動化アプリケーションです。これは、Cisco のお客様に、クロスドメイン自動化機能を提供する権限を提供します。カスタムおよび既作成の自動化テンプレートと、Cisco が提供またはシスコが独自に構築するさまざまなアダプタオプションを使用して、Cisco アプリケーションとサードパーティアプリケーションの両方でエラーが

発生しやすい反復的なタスクを合理化して、クラウドまたはオンプレミスのターゲットに到達します。

セキュリティ アプリケーション

- **Duo Security**：Cisco Duo は、すべてのユーザー、デバイス、およびアプリケーションを対象に、機密データへのアクセスを保護する二要素認証を備えた、ユーザー中心のゼロトラストセキュリティプラットフォームです。適応型ポリシー、シングルサインオン（SSO）、高度なエンドポイントの可視性などの機能を提供する、リモートアクセスの保護と事業継続性の維持のための包括的なソリューションです。
- **Cisco Secure Access**：Cisco Secure Access は、単一のクラウド管理コンソール、統合クライアント、一元化されたポリシー作成、および集約されたレポート作成機能によって IT の運用を簡素化します。1つのソリューションに統合された広範なセキュリティ機能（ZTNA、SWG、CASB、FWaaS、DNS セキュリティ、RBI など）により、ゼロトラストの原則を適用し、きめ細かいセキュリティポリシーを適用することで、セキュリティリスクを軽減します。市場をリードする Talos 脅威インテリジェンスによって比類のない脅威ブロッキングが促進され、リスクを軽減し、迅速な調査を可能にします。
- **Cisco Secure Endpoint**：Cisco Secure Endpoint（旧 Cisco AMP for Endpoints）は、侵害を防止し、脅威を迅速に検出、封じ込め、修復するように設計されたクラウド管理型のエンドポイント セキュリティ ソリューションです。高度な追跡機能を備えたクラウドベースのスキャナでファイルを即座にチェックできます。これらの機能により、セキュリティアナリストは初期のアウトブレイクソースを識別して隔離できます。このソリューションでは、悪意のあることがわかったファイルのレトロスペクティブ検疫も提供されます。
- **Cisco Security Provisioning and Administration**：Cisco 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中央管理するための Web アプリケーションです。Security Cloud Control 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 ID プロバイダーの統合などのタスクを実行できます。
- **Cisco XDR**：Cisco XDR は、セキュリティ運用を簡素化し、セキュリティチームが高度な脅威を検出、優先順位付けし、対応できるように設計されたクラウドベースのソリューションです。シスコとサードパーティの両方のセキュリティソリューションを統一されたプラットフォームに統合することで、Cisco XDR は脅威管理のための包括的なアプローチを提供します。Talos が提供する脅威インテリジェンスとの統合により、Cisco XDR は追加のコンテキストや資産に関するインサイトを使用してインシデントデータを強化し、誤検出を減らし、脅威検出、対応、およびフォレンジック機能全般を強化します。

組織の通知設定

Security Cloud Control ツールバーで、通知ボタン  をクリックします。

組織に関連付けられているすべてのユーザーには、これらのアラートが自動的に通知されます。また、これらのアラートの一部またはすべてを自分宛の電子メールに転送することができます。

（注） これらの設定を変更するには、**上位管理者**のユーザーロールが必要です。

電子メールサブスクライバ

Security Cloud Control テナントからアラートを受信する電子メールを追加または変更します。詳細については、電子メールサブスクライバの有効化 （12 ページ）を参照してください。

サービス統合

メッセージングアプリで**着信ウェブフックを有効**にし、アプリダッシュボードで直接 Security Cloud Control 通知を受信します。詳細については、「Security Cloud Control 通知のサービス統合の有効化」を参照してください。

電子メールサブスクライバの有効化

Security Cloud Control からの電子メール通知には、アクションのタイプと影響を受けるデバイスが示されます。

デバイスの現在の状態とアクションの内容の詳細については、Security Cloud Control にログインし、影響を受けるデバイスの変更ログを調べることをお勧めします。

警告 メーラーを追加する場合は、正しい電子メールを入力してください。Security Cloud Control は、テナントに関連付けられている既知のユーザーに対して電子メールアドレスをチェックしません。

電子メールサブスクリプションの追加

始める前に

電子メールサブスクリプションリストを表示するには[管理者（Admin）]、電子メールサブスクリプションを追加、削除、または編集するには [ネットワーク管理者（SuperAdmin）] である必要があります。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
ステップ 2 左側のペインで **Administration** > **Notification Settings** をクリックします。
ステップ 3 ページの右上隅にある + アイコンをクリックします。

ステップ 4 テキストフィールドに有効な電子メールアドレスを入力します。

ステップ 5 サブスクライバに通知するイベントとアラートに応じて、適切なチェックボックスをオンまたはオフにします。

ステップ 6 [保存（Save）] をクリックします。[Cancel] をクリックすることで、いつでもテナントの新しい電子メールサブスクリプションの作成を中止できます。

電子メールサブスクリプションの編集

始める前に

電子メールサブスクリプションリストを表示するには[管理者（Admin）]、電子メールサブスクリプションを追加、削除、または編集するには [ネットワーク管理者（SuperAdmin）] である必要があります。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Administration** > **Notification Settings** をクリックします。

ステップ 3 電子メールサブスクリプションの編集を有効にする電子メールアドレスを見つけます。

ステップ 4 [Edit] アイコンをクリックします。

ステップ 5 設定された電子メールアドレスにアラートを送信するには、Security Cloud Control の次の属性を編集します。

- **電子メール アドレス（Email address）**
- **デバイスのワークフロー**
- **デバイスのイベント**
- **イベントログレポート**

ステップ 6 [OK] をクリックします。[キャンセル（Cancel）] をクリックすれば、いつでも電子メールサブスクリプションに加えた変更を取り消せます。

電子メールサブスクリプションの削除

電子メールサブスクリプションリストからメーラーを削除するには、次の手順を使用します。

始める前に

電子メールサブスクリプションリストを表示するには[管理者（Admin）]、電子メールサブスクリプションを追加、削除、または編集するには [ネットワーク管理者（SuperAdmin）] である必要があります。

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
ステップ 2 左側のペインで **Administration** > **Notification Settings** をクリックします。
ステップ 3 テナントの電子メールサブスクリプションから削除するユーザーを見つけます。
ステップ 4 削除するユーザーの [削除（Remove）] アイコンをクリックします。
ステップ 5 サブスクリプションリストからユーザーを削除することを確認します。ユーザーを削除しても、ユーザーの機能にはまったく影響しません。

Security Cloud Control 通知用サービス統合の有効化

サービス統合を有効にして、指定されたメッセージングアプリケーションまたはサービスを介して Security Cloud Control 通知を転送します。通知を受信するには、メッセージング アプリケーションから Webhook URL を生成し、Security Cloud Control の [通知設定（Notification Settings）] ページでその Webhook を Security Cloud Control に指定する必要があります。

Security Cloud Control は、サービス統合として Cisco Webex、Microsoft Teams、および Slack をネイティブにサポートしています。これらのサービスに送信されるメッセージは、チャネルと自動ボット用に特別にフォーマットされています。

（注） ウェブフックごとに受信する通知の該当するボックスをオンにする必要があります。

Webex チームの着信ウェブフック

始める前に

Security Cloud Control 通知は、指定されたワークスペースに表示されるか、自動ボットとしてプライベートメッセージに表示されます。この手順を完了するには、次が必要になります。

- Webex アカウント
- Security Cloud Control アカウントとテナント

次の手順を使用して、Webex Teams の着信ウェブフックを許可します。

手順

ステップ 1 Webex AppHub [英語] を開きます。
ステップ 2 ページの上部にある [接続（Connect）] をクリックします。
ステップ 3 ページの一番下までスクロールし、次のように設定します。

- [ウェブフック名（Webhook name）]：このアプリケーションによって提供されるメッセージを識別するための名前を指定します。
- [スペースの選択（Select a space）]：ドロップダウンメニューを使用して Webex の [スペース（Space）] を選択します。このスペースは Webex チームの既存のスペースである必要があり、そのスペースへのアクセス権が必要です。スペースが存在しない場合は、Webex Teams で新しいスペースを作成できます。アプリケーションの設定ページを更新すると新しいスペースが表示されます。

（注）
過去に設定したことがある Webex の着信ウェブフックを再度有効にする場合、以前のウェブフックはこのページの下部に保持されています。以前のウェブフックが不要になった場合、または Webex スペースが存在しなくなった場合は、以前のウェブフックを削除できます。

ステップ 4 [追加（Add）] を選択します。選択した Webex スペースに、アプリケーションが追加されたという通知が送信されます。

ステップ 5 ウェブフック URL をコピーします。

ステップ 6 Security Cloud Control にログインします。

ステップ 7 左側のペインで **Administration** > **Notification Settings** をクリックします。

ステップ 8 適切な通知がチェックされていることを確認します。そうでない場合は、サービス統合に接続する前に通知の選択内容を変更することを強く推奨します。

ステップ 9 [サービス統合（Service Integrations）] までスクロールします。

ステップ 10 青色のプラスボタンをクリックします。

ステップ 11 名前を入力します。 この名前は、設定されたサービス統合として Security Cloud Control に表示されます。設定されたサービスに転送されるイベントには表示されません。

ステップ 12 ドロップダウンメニューを展開し、サービスタイプとして Webex を選択します。

ステップ 13 サービスから生成したウェブフック URL を貼り付けます。

ステップ 14 [OK] をクリックします。

Microsoft Teams 用着信ウェブフック

Security Cloud Control は Microsoft Teams に通知を転送できます。これらのメッセージは、指定されたチャンネルに表示されるか、Microsoft Teams のプライベート チャット メッセージに自動ボットとして表示されます。この機能を有効にするには、Microsoft Teams からウェブフック URL を生成し、そのウェブフックを Security Cloud Control で指定する必要があります。Microsoft Teams チャンネルへの受信ウェブフックの追加に関する詳細については、「Microsoft Teams のワークフローを使用した受信ウェブフックの作成」を参照してください。

前提条件

Microsoft Teams で Security Cloud Control 通知を許可する前提条件は次のとおりです。

- Microsoft Teams アカウント。
- Security Cloud Control アカウントとテナント

Microsoft Teams でウェブフック URL を生成し、Security Cloud Control からの通知を有効にするには、次の手順を実行します。

手順

ステップ 1 Microsoft Teams アカウントにログインします。

ステップ 2 **[New Teams]** クライアントで、**[Teams]** をクリックし、着信ウェブフックを追加するチャンネルに移動します。

ステップ 3 チャンネル名の横にある **[More options •••]** をクリックします。

ステップ 4 [ワークフロー（Workflows）] をクリックします。

ステップ 5 **[Post to a channel when a webhook request is received]** をクリックします。

ステップ 6 ウェブフック名を入力し、**[Next]** をクリックします。

ステップ 7 通知を送信する必要があるチャネルを選択します。

Microsoft Teams のチャットまたはチャンネルからこのワークフローを使用する場合、これらのフィールドは自動的に入力されます。

ステップ 8 必要な詳細を入力した後、**[Add workflow]** をクリックします。

ステップ 9 表示されるダイアログボックスから一意のウェブフック URL をコピーします。URL はチャンネルにマッピングされます。これを使用して、Teams に情報を送信できます。

ステップ 10 Cisco Security Cloud Control にログインします。

ステップ 11 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 12 左側のペインから、**[Platform Management]** > **[Notification Settings]**をクリックします。

ステップ 13 [サービス統合（Service Integrations）] までスクロールします。

ステップ 14 青色のプラスボタンをクリックします。

ステップ 15 名前を入力します。

この名前は、Security Cloud Control に設定されたサービス統合として表示されます。しかし、設定されたサービスに転送されるイベントには表示されません。

ステップ 16 ドロップダウンメニューを展開し、**Microsoft Teams** を **[Service Type]** として選択します。

ステップ 17 Microsoft Teams から生成したウェブフック URL を **URL** に貼り付けます。

ステップ 18 **[Send Alerts When]** で、選択した通知が正しいことを検証し、確認します。通知されない場合は、続行する前に通知の選択を変更してください。

ステップ 19 [Save] をクリックします。

Slack 用の着信ウェブフック

Security Cloud Control 通知は、指定されたチャネルに表示されるか、自動ボットとしてプライベートメッセージに表示されます。Slack による着信ウェブフックの処理方法の詳細については、「Slack Apps」を参照してください。

次の手順を使用して、Slack の着信ウェブフックを許可します。

手順

ステップ 1 Slack アカウントにログインします。

ステップ 2 左側のパネルで、一番下までスクロールして [アプリの追加（Add Apps）] を選択します。

ステップ 3 [着信ウェブフック（Incoming Webhooks）] のアプリケーション ディレクトリを検索し、アプリを見つけます。[追加（Add）] を選択します。

ステップ 4 Slack ワークスペースの管理者ではない場合、組織の管理者にリクエストを送信し、アプリが自分のアカウントに追加されるのを待つ必要があります。[設定のリクエスト（Request Configuration）] を選択します。オプションのメッセージを入力し、[リクエストの送信] を選択します。

ステップ 5 ワークスペースで着信ウェブフックアプリが有効になったら、Slack の設定ページを更新し、[新しいウェブフックをワークスペースに追加（Add New Webhook to Workspace）] を選択します。

ステップ 6 ドロップダウンメニューを使用して、Security Cloud Control 通知を表示する Slack チャネルを選択し、[承認（Authorize）] を選択します。リクエストが有効になるのを待っている間にこのページから移動した場合は、Slack にログインして、左上隅にあるワークスペース名を選択します。ドロップダウンメニューから [ワークスペースのカスタマイズ（Customize Workspace）] を選択し、[アプリの設定（Configure Apps）] を選択します。**[管理（Manage）]** > **[カスタム統合（Custom Integrations）]** に移動します。**[Incoming Webhooks]** を選択してアプリのランディングページを開き、タブから **[Configuration]** を選択します。このアプリが有効になっているワークスペース内のすべてのユーザーが一覧表示されます。ユーザーはアカウントの設定の表示と編集のみできます。ワークスペース名を選択して設定を編集し、次に進みます。

ステップ 7 Slack の設定ページから、アプリの設定ページにリダイレクトされます。ウェブフック URL を見つけてコピーします。

ステップ 8 Security Cloud Control にログインします。

ステップ 9 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 10 左側のペインで **Administration** > **Notification Settings** をクリックします。

ステップ 11 適切な通知がチェックされていることを確認します。そうでない場合は、サービス統合に接続する前に通知の選択内容を変更することを強く推奨します。

ステップ 12 [サービス統合（Service Integrations）] までスクロールします。

ステップ 13 青色のプラスボタンをクリックします。

ステップ 14 名前を入力します。 この名前は、設定されたサービス統合として Security Cloud Control に表示されます。設定されたサービスに転送されるイベントには表示されません。

ステップ 15 ドロップダウンメニューを展開し、サービスタイプとして [Slack] を選択します。

ステップ 16 サービスから生成したウェブフック URL を貼り付けます。

ステップ 17 [OK] をクリックします。

カスタム統合用の着信ウェブフック

始める前に

Security Cloud Control は、カスタム統合用にメッセージをフォーマットしません。カスタムサービスまたはアプリケーションの統合を選択した場合、Security Cloud Control は JSON メッセージを送信します。

着信ウェブフックを有効にしてウェブフック URL を生成する方法については、サービスのマニュアルを参照してください。ウェブフック URL を取得したら、以下の手順を使用してウェブフックを有効にします。

手順

ステップ 1 選択したカスタムサービスまたはアプリケーションからウェブフック URL を生成してコピーします。

ステップ 2 Security Cloud Control にログインします。

ステップ 3 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 4 左側のペインで **Administration** > **Notification Settings** をクリックします。

ステップ 5 適切な通知がチェックされていることを確認します。そうでない場合は、サービス統合に接続する前に通知の選択内容を変更することを強く推奨します。

ステップ 6 [サービス統合（Service Integrations）] までスクロールします。

ステップ 7 青色のプラスボタンをクリックします。

ステップ 8 名前を入力します。 この名前は、設定されたサービス統合として Security Cloud Control に表示されます。設定されたサービスに転送されるイベントには表示されません。

ステップ 9 ドロップダウンメニューを展開し、[サービスタイプ（Service Type）] として [カスタム（Custom）] を選択します。

ステップ 10 サービスから生成したウェブフック URL を貼り付けます。

ステップ 11 [OK] をクリックします。

ロギングの設定

毎月のイベントロギングの制限と、制限がリセットされるまでの残り日数を表示します。保存されたロギングは、Cisco Cloud が受信した圧縮されたイベントデータを表すことに注意してください。

[View Historical Usage] をクリックして、過去 12 か月間にテナントで受信されたログを表示します。

追加のストレージをリクエストするために使用できるリンクもあります。

SAML シングルサインオンと Security Cloud Control の統合

Security Cloud Control は、Cisco Secure Sign-On を SAML シングル サインオン アイデンティティ プロバイダー（IdP）として使用し、多要素認証（MFA）に Duo Security を使用します。これは、Security Cloud Control で推奨される認証方法です。

ただし、顧客が独自の SAML シングルサインオン IdP ソリューションと Security Cloud Control を統合したい場合、IdP が SAML 2.0 および ID プロバイダーが開始するワークフローをサポートしている限り、それも可能です。

独自またはサードパーティのアイデンティティ プロバイダー（IdP）を Cisco Security Cloud Sign On と統合するには、『Cisco Security Cloud Sign On Identity Provider Integration Guide』を参照してください。

独自の SAML ソリューションを Security Cloud Control と統合する必要がある場合は、サポートに連絡してケースを作成してください。

注目 ケースを開く場合は、[テクノロジーを手動で選択（Manually Select A Technology）] を選択し、リクエストが適切なチームに到達するように [SecureX - サインオンと管理（SecureX - Sign-on and Administration）] を選択していることを確認してください。

SSO 証明書の更新

通常、ID プロバイダー（IdP）は SecureX SSO と統合されています。Cisco TAC ケースを開き、metadata.xml ファイルを提供します。詳細については、『Cisco SecureX Sign-On Third-Party Identity Provider Integration Guide』を参照してください。

注目 ケースを開く場合は、[テクノロジーを手動で選択（Manually Select A Technology）] を選択し、リクエストが適切なチームに到達するように [SecureX - サインオンと管理（SecureX - Sign-on and Administration）] を選択していることを確認してください。

（レガシーのみ）アイデンティティ プロバイダー（IdP）が Security Cloud Control と直接統合されている場合は、Security Cloud Control TAC でサポートチケットを開き、metadata.xml ファイルを提供します。

マイトークン

詳細については、「API トークン」を参照してください。

API トークン

開発者は、Security Cloud Control REST API 呼び出しを行うときに Security Cloud Control API トークンを使用します。呼び出しを成功させるには、API トークンを REST API 認証ヘッダーに含める必要があります。API トークンは「長期」アクセストークンとして機能し、有効期限はありませんが、更新または取り消すことが可能です。

Security Cloud Controlで API トークンを生成するには、最初に API 専用ユーザーを作成する 必要があります（まだ存在しない場合）。このユーザーは、API トークンの生成と使用のために特別に指定されています。

API 専用ユーザーを作成すると、そのユーザー用に新しい API トークンを生成できます。トークンは生成された直後にのみ表示され、**[General Settings]** ページに移動している間は表示されたままになります。別のページを開いてから **[General Settings]** ページに戻ると、トークンが発行されたことはわかりますが、トークンは表示されなくなります。

（注） API 専用ユーザーは API トークンを生成できます。個人ユーザーは自分自身または他のユーザー用に API トークンを作成できません。

API トークン形式とクレーム

API トークンは JSON Web トークン（JWT）です。JWT トークン形式の詳細については、「Introduction to JSON Web Tokens」を参照してください。

Security Cloud Control API トークンは、次の一連のクレームを提供します。

- **id**：ユーザー/デバイス uid
- **parentId**：テナント uid
- **ver**：公開キーのバージョン（初期バージョンは 0、例：**cdo_jwt_sig_pub_key.0**）
- **subscriptions**：Security Services Exchange サブスクリプション（任意）
- **client_id**：「**api-client**」
- **jti**：トークン id

Security Cloud Control の API 専用ユーザーの管理

API 専用ユーザーロールを使用すると、ユーザーはユーザーインターフェイスなしで API を使用して Security Cloud Control を操作できます。API 専用ユーザーロールは、自動化されたプロセスと統合が必要な組織で役立ちます。

API 専用ユーザーのアクセスを管理するには、次の手順を実行します。

1. Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
2. 左側のペインで、**Administration** > **API User Management** を選択します。

他のユーザーへのアクセスを許可する、ユーザーロールを変更する、または新しいユーザーを招待するには、次の手順を実行します。

1. Security Cloud Control ホームページから、 **[Platform Services]** > **[Platform Management]** を選択します。Security Cloud Control ホームページで、 の順に選択します。
2. **[アクセス管理（Access Management）]** > **[管理者アクセス（Administrator Access）]** を選択します。

   詳細については、Security Cloud Control プラットフォームサービスの「ユーザーの管理」を参照してください。

トークンの管理

API のみのユーザーを作成する

ユーザーの作成時に、スーパー管理者は [APIのみのユーザー（API Only User）] を選択して仮想ユーザータイプを作成し、Security Cloud Control REST API 呼び出しを行うときに Security Cloud Control を認証するための API トークンを生成できます。Security Cloud Control では、E メールアドレスの代わりにユーザー名を入力するように求められます。これにより、元のスーパー管理者が組織を離れた後でも権限が引き続き機能します。API のみのユーザーは Security Cloud Control インターフェイスにログインできません。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 **[Add a new user]**（  ）アイコンをクリックして、新しいユーザーをテナントに追加します。

ステップ 5 [APIのみのユーザー（API Only User）] チェックボックスを選択します。

ステップ 6 [ユーザー名（Username）] フィールドに ユーザー名を入力し、[OK] をクリックします。

重要
ユーザー名に E メールアドレスを使用したり、「@」文字を含めることはできません。「@yourtenant」サフィックスがユーザー名に自動的に追加されるためです。

ステップ 7 ドロップダウンメニューからユーザーのロールを選択します。

ステップ 8 [OK] をクリックします。

API トークンの生成

Security Cloud Control APIを使用するには、API トークンが必要です。Security Cloud Control テナントに API専用ユーザーを作成し、そのユーザー用のトークンを生成することを推奨します。

このトークンは、REST API コールの認証ヘッダーで使用される有効期間の長いベアラートークンです。同じトークンが Security Cloud Control API とクラウド提供型 Firewall Management Center API の両方に使用されます。

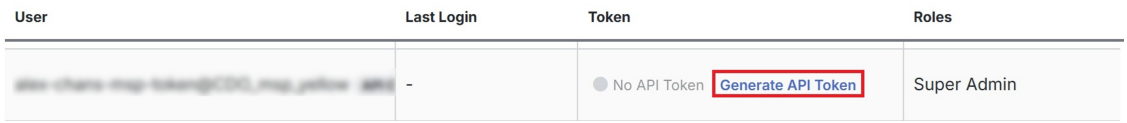
手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 **[Token]** 列の下にある **[Generate API Token]** をクリックします。



ステップ 5 機密データを取り扱うための企業のベストプラクティスに従って、トークンを安全な場所に保存します。

次のタスク

詳細については、「Cisco Security Cloud Control ファイアウォール API ドキュメントのスタートアップガイド」を参照してください。

API トークンの更新

API トークンに有効期限はありませんが、ユーザーは、トークンが紛失した場合、侵害された場合、または企業のセキュリティガイドラインに準拠させる場合、既存の API トークンを更新させることで API トークンの更新を選択できます。

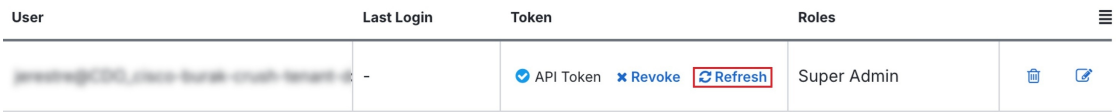
手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 **[Token]** 列の下の **[Refresh]** をクリックします。Security Cloud Control は新しい API トークンを生成します。



ステップ 5 機密データを維持するための企業のベストプラクティスに従って、新しいトークンを安全な場所に保存します。

（注）
Dynamic Attributes Connector サービスアカウント（csdac-service@tenantname）の API 専用ユーザーの、**[Revoke]**、**[Refresh]**、**[Delete]**、および **[Edit]** オプションが無効になっています。これは、ユーザーが Dynamic Attributes Connector の機能に必要な、この API アカウントの API トークンを削除、編集、または取り消しないようにするためです。

API トークンの取り消し

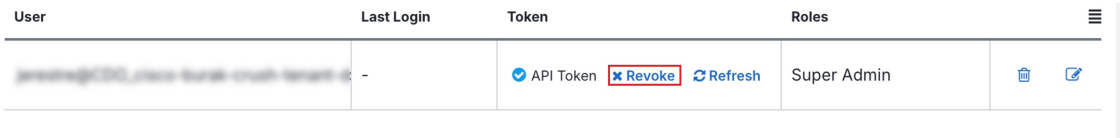
手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 **[Token]** 列で、API トークンを生成するユーザーの **[Revoke]** をクリックします。



（注）
Dynamic Attributes Connector サービスアカウント（csdac-service@tenantname）の API 専用ユーザーの、**[Revoke]**、**[Refresh]**、**[Delete]**、および **[Edit]** オプションが無効になっています。これは、ユーザーが Dynamic Attributes Connector の機能に必要な、この API アカウントの API トークンを削除、編集、または取り消しないようにするためです。

アイデンティティ プロバイダー アカウントと Security Cloud Control ユーザーレコードとの関係

Security Cloud Control にログインするには、SAML 2.0 準拠の ID プロバイダー（IdP）、多要素認証プロバイダー、および Security Cloud Control のユーザーレコードを持つアカウントが必要です。IdP アカウントにはユーザーのログイン情報が含まれており、IdP はそのログイン情報に基づいてユーザーを認証します。多要素認証では、アイデンティティセキュリティの付加的なレイヤが提供されます。Security Cloud Control ユーザーレコードには、主にユーザー名、ユーザーが関連付けられる Security Cloud Control テナント、ユーザーのロールが含まれます。ユーザーがログインすると、Security Cloud Control は IdP のユーザー ID を Security Cloud Control の

テナントの既存ユーザーレコードにマッピングします。Security Cloud Control が一致するレコードを見つけた場合に、該当するユーザーはそのテナントへのログインを許可されます。

お客様の企業に独自のシングルサインオン ID プロバイダーがない限り、ID プロバイダーは Cisco Security Cloud Sign On です。Cisco Security Cloud Sign On は、多要素認証に Duo を使用します。お客様は、必要に応じて自分の IdP を Security Cloud Control と統合できます。

ログインのワークフロー

ここでは、IdP アカウントが、Security Cloud Control ユーザーにログインするために Security Cloud Control ユーザーレコードとどのようにやり取りするかについて簡単に説明します。

手順

ステップ 1 ユーザーは、認証のために Cisco Security Cloud Sign On（https://security.cisco.com）などの SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）にログインして、Security Cloud Control へのアクセスを要求します。

ステップ 2 IdP は、ユーザーが本人であることを示す SAML アサーションを発行し、ポータルには、ユーザーがアクセスできるアプリケーションが表示されます。そのタイルの 1 つが Security Cloud Control です。

ステップ 3 Security Cloud Control は SAML アサーションを検証し、ユーザー名を抽出して、そのユーザー名に対応するテナントの中からユーザーレコードを見つけようとします。

- ユーザーが Security Cloud Control 上の 1 つのテナントにユーザーレコードを持っている場合、Security Cloud Control はそのユーザーにテナントへのアクセスを許可し、ユーザーロールによって実行できるアクションが決まります。
- ユーザーが複数のテナントにユーザーレコードを持っている場合、Security Cloud Control は認証されたユーザーに、選択できるテナントのリストを提示します。ユーザーがテナントを選択すると、テナントへのアクセスが許可されます。その特定のテナントでのユーザーロールによって、実行できるアクションが決まります。
- 認証されたユーザーとテナントのユーザーレコードとのマッピングが Security Cloud Control にない場合、Security Cloud Control はランディングページを表示して、ユーザーに Security Cloud Control の詳細を確認したり、無料試用版をリクエストしたりする機会を提供します。

Security Cloud Control でユーザーレコードを作成しても IdP にアカウントは作成されず、IdP でアカウントを作成しても Security Cloud Control にユーザーレコードは作成されません。

同様に、IdP のアカウントを削除しても、Security Cloud Control からユーザーレコードを削除したことにはなりません。ただし、IdP アカウントがないと、Security Cloud Control に対してユーザーを認証する方法はありません。Security Cloud Control ユーザーレコードの削除は、IdP アカウントを削除したことを意味するものではありません。ただし、Security Cloud Control ユーザー

レコードがなければ、認証されたユーザーが Security Cloud Control テナントにアクセスする方法はありません。

このアーキテクチャの影響

Cisco Security Cloud Sign On を使用するお客様

お客様が Security Cloud Control の Cisco Security Cloud Sign On ID プロバイダーを使用している場合、スーパー管理者は Security Cloud Control でユーザーレコードを作成でき、ユーザーは Security Cloud Control に自己登録できます。2 つのユーザー名が一致し、ユーザーが正しく認証されている場合、ユーザーは Security Cloud Control にログインできます。

ユーザーが Security Cloud Control にアクセスできないようにする必要がある場合は、スーパー管理者が Security Cloud Control ユーザーのユーザーレコードを削除するだけで済みます。Cisco Security Cloud Sign On アカウントは引き続き存在し、スーパー管理者がユーザーを復元したい場合は、Cisco Security Cloud Sign On で使用していたものと同じユーザー名で新しい Security Cloud Control ユーザーレコードを作成することができます。

お客様が Security Cloud Control の問題に遭遇し、テクニカル アシスタンス センター（TAC）を呼び出す必要が生じた場合、お客様が TAC エンジニアのユーザーレコードを作成することで、TAC エンジニアがテナントを調査し、お客様に情報と提案を報告できるようになります。

独自のアイデンティティ プロバイダーをもつ顧客

独自のアイデンティティ プロバイダーを持つお客様は、アイデンティティ プロバイダー アカウントと Security Cloud Control テナントの両方を制御します。このようなお客様は、Security Cloud Control でアイデンティティ プロバイダーのアカウントとユーザーレコードを作成および管理できます。

ユーザーが Security Cloud Control にアクセスできないようにする必要がある場合は、お客様は IdP アカウント、Security Cloud Control ユーザーレコード、またはその両方を削除できます。

Cisco TAC からの支援が必要な場合は、お客様は読み取り専用ロールを持つアイデンティティ プロバイダー アカウントと Security Cloud Control ユーザーレコードの両方を、TAC エンジニア用に作成できます。TAC エンジニアは、お客様の Security Cloud Control テナントにアクセスして調査し、情報と提案をお客様に報告することができます。

シスコ マネージドサービス プロバイダー

シスコ マネージドサービス プロバイダー（MSP）は、Security Cloud Control の Cisco Security Cloud Sign On IdP を使用している場合、Cisco Security Cloud Sign On に自己登録できます。MSP のお客様は Security Cloud Control にそれぞれのユーザーレコードを作成できるため、MSP はお客様のテナントを管理できます。もちろん、お客様は MSP のレコードの削除を完全に制御できます（削除を選択した場合）。

関連項目

- 全般設定

- [ユーザー管理（User Management）]
- Security Cloud Control ユーザーロール

MSSP ポータル

Security Cloud Control の MSSP ポータルは、複数のテナント間でデバイスを効率的にモニターおよび管理するためのマネージド セキュリティ サービス プロバイダー（MSSP）向けのマルチテナントのクラウドベースの管理プラットフォームです。

このポータルでは、**設定ステータス**、**接続状態**、**ソフトウェアバージョン**、および全体的なネットワークの正常性などのリアルタイム情報が単一のインターフェイスに統合され、個々のテナント環境にアクセスすることなく、シームレスな概要が提供されます。

はじめる前に

- Cisco TAC でサポートチケットを開き、テナントを管理するための MSSP ポータルを作成します。詳細については、TAC でサポートチケットを開くを参照してください。
- 特定のブラウザ関連の問題を回避するために、Web ブラウザからキャッシュと Cookie をクリアすることをお勧めします。

MSSP ポータルコンポーネント

ポータルの左側のペインに表示されるオプションを使用すると、ポータル内のセキュリティデバイスとテナントに関する詳細を表示したり、ポータル設定を設定したりできます。

- **Dashboard**
  - **[General overview]** では、デバイス、クラウドサービス、およびファイアウォールマネージャの概要とその接続ステータスが一目で確認できます。この機能は、問題がある可能性のあるデバイスを迅速に特定するのに役立ちます。
  - **[Health overview]** では、テナントにオンボードされた Secure Firewall ASA デバイスの重要なパフォーマンスデータに関するインサイトが提供されます。

    詳細については、「MSSP ポータルでの正常性の概要ダッシュボードの表示」を参照してください。

- **セキュリティ デバイス**

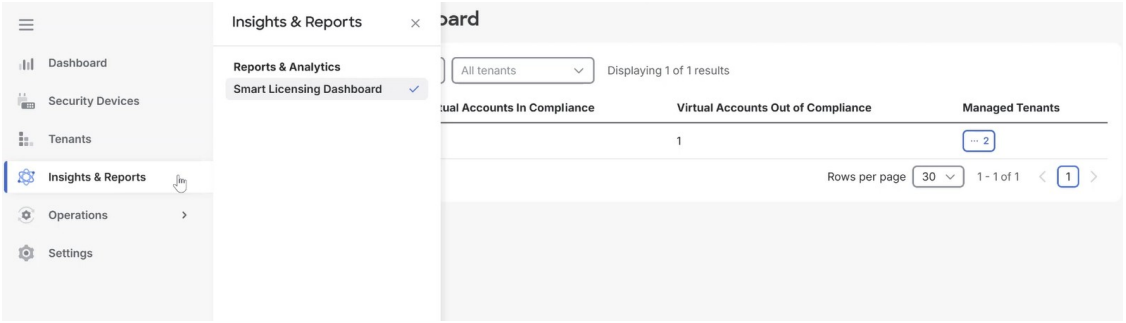
  ポータルに追加されたテナントにオンボードされたすべてのデバイス、クラウドサービス、テンプレート、およびファイアウォールマネージャに関する情報を提供します。詳細については、セキュリティデバイスの詳細 （28 ページ）を参照してください。

- **テナント**
  - ポータルによって管理されるすべてのテナントに関する情報を提供します。テナント名で検索したり、テナントの情報をカンマ区切り値（CSV）ファイルにエクスポートしたりできます。

- ポータルに新しいテナントを作成するか、既存のテナントを追加できるのは、**ネットワーク管理者**権限を持つユーザーのみであることに注意してください。

- **インサイトとレポート**

  スマート ライセンシング ダッシュボードは、Secure Firewall ASA および Cloud-Delivered Firewall Management Center 管理対象Secure Firewall Threat Defenseデバイスのライセンス使用状況とコンプライアンスステータスを可視性として表示します。



- **動作（Operations）**

  [Upgrades] 機能を使用すると、複数の管理対象組織にわたって Cloud-Delivered Firewall Management Center（cdFMC）によって管理される複数の Secure Firewall Threat Defense デバイスをアップグレードできます。

（注） マルチテナントデバイスのアップグレードはベータ機能です。

- **設定**

  - **[General Settings] では、ポータル設定**に関する情報が表示されます。
  - [User Management] では、すべての [Users]、[Active Directory Groups]、および [Audit Logs] のリストを表示できます。詳細については、「ユーザーの管理」を参照してください。

（注） ネットワーク管理者権限を持つユーザーの場合、APIエンドポイントを使用して次の操作を実行できます。

- Security Cloud Control テナントの作成
- 既存の Security Cloud Control テナントのマルチテナントポータルへの追加

セキュリティデバイスの詳細

左側のペインで **[Security Devices]** をクリックすると、次のタブを含む **[Security Devices]** ページが表示されます。

表 *1:* セキュリティデバイスページのタブの説明

タブ名	説明
デバイス	ポータルに追加されたテナントにオンボード済みのすべてのデバイスが表示されます。 • デバイスをクリックすると、**デバイスの詳細**、**テナントの詳細**、および**アクション**が表示されます。 • **[Actions]** の下の**[Manage Device on Tenant]** をクリックすることで、Security Cloud Control でこのデバイスを管理できます。そのテナントのアカウントを持っており、テナントとポータルが同じリージョン内にある場合に、このリンクが表示されます。テナントにアクセスする権限がない場合は、**[Manage Device on Tenant]** リンクは表示されません。権限については、組織のネットワーク管理者にお問い合わせください。 • **[Filters]** をクリックして、**[Device/Services]**、**[Configuration Status]**、**[Connectivity State]**、**[Software Version]**、**[Tenant]**、または **[Conflict Detection]**でデバイスをフィルタ処理します。
クラウド サービス（**Cloud Services**）	ポータル内のテナントにオンボードされているすべてのクラウドサービスを表示します。 • クラウドサービスをクリックすると、**デバイスの詳細**、**テナントの詳細**、および**アクション**が表示されます。 • **[Filters]** をクリックして、**[Services]**、**[Configuration Status]**、**[Connectivity State]**、**[Tenant]**、**[Conflict Detection]** でデバイスをフィルタ処理します。

タブ名	説明
テンプレート	ポータル内のテナントにオンボードされているすべてのテンプレートを表示します。 • テンプレートをクリックすると、**デバイスの詳細**、**テナントの詳細**、および**アクション**が表示されます。 • **[Filters]** をクリックして、**[Template Type]**、**[Configuration Status]**、**[Software Version]**、または **[Tenant]** でデバイスをクラウドサービス処理します。
ファイアウォールマネージャ	ポータル内のテナントにオンボードされているすべてのファイアウォールマネージャを表示します。 • ファイアウォールマネージャをクリックして、**デバイスの詳細**、**テナントの詳細**、および **アクション**を表示します。 • **[Filters]** をクリックして、**[Device Managers]**、**[Connectivity State]**、**[Tenant]** または **[Software Version]** でクラウドサービスをフィルタ処理します。

- 詳細をカンマ区切り値（.csv）ファイルにエクスポートして、分析およびコンプライアンスレポートに役立てることができます。データをエクスポートするたびに、Security Cloud Control では新しい .csv ファイルが作成されます。このファイルには、作成タイムスタンプとポータルの汎用一意の識別子がファイル名に含まれています。
- 列ピッカーを使用して、テーブルに表示するデバイスプロパティを選択またはクリアできます。テーブルの右上隅にある歯車アイコン（⚙）をクリックし、[Table Settings] を編集します。

  テーブルをカスタマイズすると、次回サインインしたとき、選択した内容が Security Cloud Control で保持されています。**[Security Devices]** ページを表示します。

MSSP ポータルにテナントを追加

ネットワーク管理者権限を持つユーザーは、複数のリージョンにわたってMSSPポータルにテナントを追加できます。たとえば、ヨーロッパから米国にテナントを追加することも、その逆を行うこともできます。

重要 テナントに API 専用のユーザーを作成し、Security Cloud Control への認証用に API トークンを生成することをお勧めします。

（注） ポータルに複数のテナントを追加する場合は、各テナントから API トークンを生成し、テキストファイルに貼り付けます。これにより、複数のテナントをポータルに簡単に追加できます。トークンを生成するために毎回テナントを切り替える必要はありません。

手順

ステップ 1 左側のペインで [テナント（Tenants）] をクリックします。

ステップ 2 ページの右上隅にある + アイコンをクリックします。

ステップ 3 新しいテナントを追加するには、[次へ（Next）] をクリックします。

（注）

1. 既存のテナントをインポートするには、[Would you like to import existing tenant?] チェックボックスをオンにします。
2. Security Cloud Control から既存のテナントを追加するには、複数の API トークンをカンマで区切って貼り付けます。
3. [インポート（Import）] をクリックします。

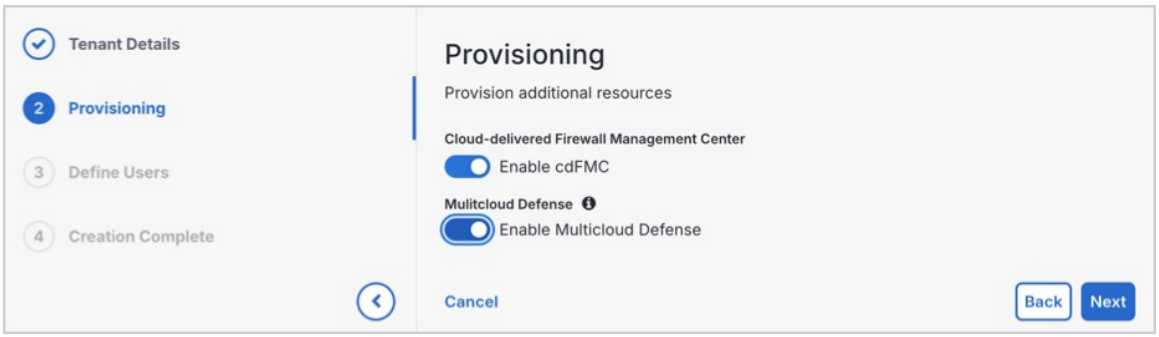
ステップ 4 [Tenant Details] で、[Display Name] と [Tenant Name] を入力します。

注： SO 番号なしでテナントを作成した場合は、30 日間の価値実証トライアルが実施されます。

ステップ 5 [Next] をクリックします。

ステップ 6 [プロビジョニング（Provisioning）] で、

- [Enable cdFMC] トグルを有効にして、テナントの Cloud-Delivered Firewall Management Center をプロビジョニングします。
- [Enable Multicloud Defense] トグルを有効にして、テナントの Multicloud Defense をプロビジョニングします。
- [Next] をクリックします。



ステップ 7 [Define Users] で、電子メールアドレスを入力して役割を選択し、ユーザーを 1 人ずつ手動で追加するか、CSV テンプレートをダウンロードし、必要な詳細を入力してファイルをアップロードします。

追加されたユーザーは、[User list] セクションに表示されます。

ステップ 8 [テナントの作成（Create Tenant）] をクリックします。

テナントの作成が完了しました。プロビジョニングには数分かかる場合があります。

MSSP ポータルからのテナントの削除

手順

ステップ 1 左側のペインで [テナント（Tenants）] をクリックします。

ステップ 2 右側の対応する削除アイコンをクリックして、テナントを削除します。

ステップ 3 [削除（Remove）] をクリックします。

このとき、関連付けられたデバイスもポータルから削除されます。

スマート ライセンシング ダッシュボードの概要

MSSP ポータルの**スマート ライセンス ダッシュボード**では、Secure Firewall ASA、および Cloud-Delivered Firewall Management Center 管理対象 Secure Firewall Threat Defense デバイスのライセンス使用状況とコンプライアンスステータスの可視性が提供されます。

スマート ライセンシング ダッシュボードのメリット

- **ライセンスの包括的な可視性**：ライセンスの発信元のスマートアカウントと仮想アカウントを確認できるため、ライセンスソースの明確なトレーサビリティが提供されます。
- **詳細なライセンス使用量の追跡**：消費しているライセンス数を、各ライセンスタイプの可用性、使用状況、および期限日とともに確認できます。

- **コンプライアンス準拠状況のモニタリング**：各ライセンスのコンプライアンス準拠状況を確認できるため、ソフトウェア利用資格の範囲内での利用を維持し、コンプライアンス違反の問題を回避することができます。

（注）
- スマートライセンスはスマートアカウントを使用して管理されます。各スマートアカウントには複数のバーチャルアカウントを作成できます。スマートアカウントの所有者は、これらの仮想アカウント間でライセンスを移動できます。
- このダッシュボードには、現在のテナントにのみ関連付けられているすべてのスマートアカウント、仮想アカウント、およびライセンスの詳細が表示されます。

スマート ライセンシング ダッシュボードの表示

MSSP ポータルの **スマート ライセンス ダッシュボード** には、ライセンスに関する詳細情報が表示されます。ダッシュボードには、準拠ステータス（**準拠**、 **非準拠**、または **不明**）、購入済みライセンス数、および現在使用中のライセンス数が、テナント内の有効なライセンス数とともに表示されます。また、オンボーディングされたデバイスに関連付けられたライセンスのタイプ（**期間**、 **未ライセンス**、または **永続的**）、および各期間ライセンスの開始日と期限日も表示されます。

手順

ステップ 1 **[Insights & Reports]** > **[Reports & Analytics]** > **[Smart Licensing Dashboard]**を選択します。

次の表に、ページに表示される情報の詳細を示します。

列名	Description
ドメイン	スマートアカウントのドメイン名。
コンプライアンスに準拠したバーチャルアカウント	このスマートアカウントドメインの下にある、準拠しているバーチャルアカウントの数。
準拠していないバーチャルアカウント	このスマートアカウントドメインの下にある、準拠していないバーチャルアカウントの数。
管理対象テナント	このスマートアカウントに関連付けられているこのテナントの管理対象テナントの名前。

ステップ 2 **[Domain]** 列の下にあるスマートアカウントドメイン名をクリックすると、この MSSP テナントの下で、このバーチャルアカウントに関連付けられているすべての管理対象テナントが表示されます。

（注）
ドロップダウンリストには、利用可能なすべてのドメインではなく、テナント内のデバイスにリンクされているスマートアカウントドメインのみが含まれます。

次の表に、ページに表示される情報の詳細を示します。

列名	Description
バーチャルアカウント名	仮想アカウントの名前。
コンプライアンスステータス	バーチャルアカウントの準拠ステータス。
テナント	この仮想アカウントに関連付けられているこのテナントの管理対象テナントの名前。

（注）
バーチャルアカウントに関連付けられている複数のテナントを使用できます。

[Smart account domain] ドロップダウンリストから、他のスマートアカウントドメインを表示するドメイン名を選択します。検索フィールドを使用して、バーチャルアカウント名、コンプライアンスステータス、またはテナント名で項目を検索することもできます。

ステップ 3 バーチャルアカウント名をクリックして詳細を表示します。

次の表に、ページに表示される情報の詳細を示します。

列名	Description
ライセンス名	スマートライセンスの名前。
Type	テナントにオンボードされたデバイスに関連付けられているライセンスのタイプ： **期限付き**、**未ライセンス**、または **永久**。
購入	購入したスマートライセンスの数。
使用中(In use)	現在使用中のスマートライセンスの数。
このテナント内	選択したテナントで使用されているスマートライセンスの数。
応対可	現在使用可能なスマートライセンスの数。
日付	有効期限付きライセンスの開始日と有効期限。
コンプライアンスステータス	準拠ステータス： **準拠**、**非準拠**、または **不明**。
テナント	このスマートライセンスに関連付けられているこのテナントの管理対象テナントの名前。

このページの検索フィールドを使用して、ライセンス名、ステータス、またはタイプでフィルタ処理できます。

ステップ 4 CSV ファイルにテーブルをエクスポートするには、[Export] をクリックします。

MSSP ポータルでのマルチテナントデバイスのアップグレードについて

MSSP ポータルを使用して、クラウド提供型ファイアウォール管理センター（cdFMC）によって管理される複数のテナントにわたる Cisco Secure Firewall Threat Defense デバイスを一括アップグレードできます。**[Operations]** ダッシュボードの **[Upgrades]** ページを使用して、MSSP ポータルのクラウド提供型ファイアウォール管理センター（cdFMC）によって管理される複数の Cisco Secure Firewall Threat Defense デバイスを選択し、アップグレードを実行できます。

（注） マルチテナントデバイスのアップグレードはベータ機能です。

マルチテナントデバイスのアップグレードの利点

- 大規模な一括アップグレードを実行するための統合ダッシュボードの可用性。
- アップグレードするバージョンを決定するのに役立つアップグレードパッケージのリストの可用性。

MSSP ポータルでのマルチテナントデバイスのフルアップグレードの開始

フルアップグレードを開始する場合は、パッケージを選択し、選択したデバイスにアップロードし、準備状況チェックを実施して、アップグレードプロセスを中断せずに完了する必要があります。

完全アップグレードを開始するには、次の手順を実行します。

手順

ステップ 1 左側のペインから、**[Operations]** > **[Upgrades]** に移動します。

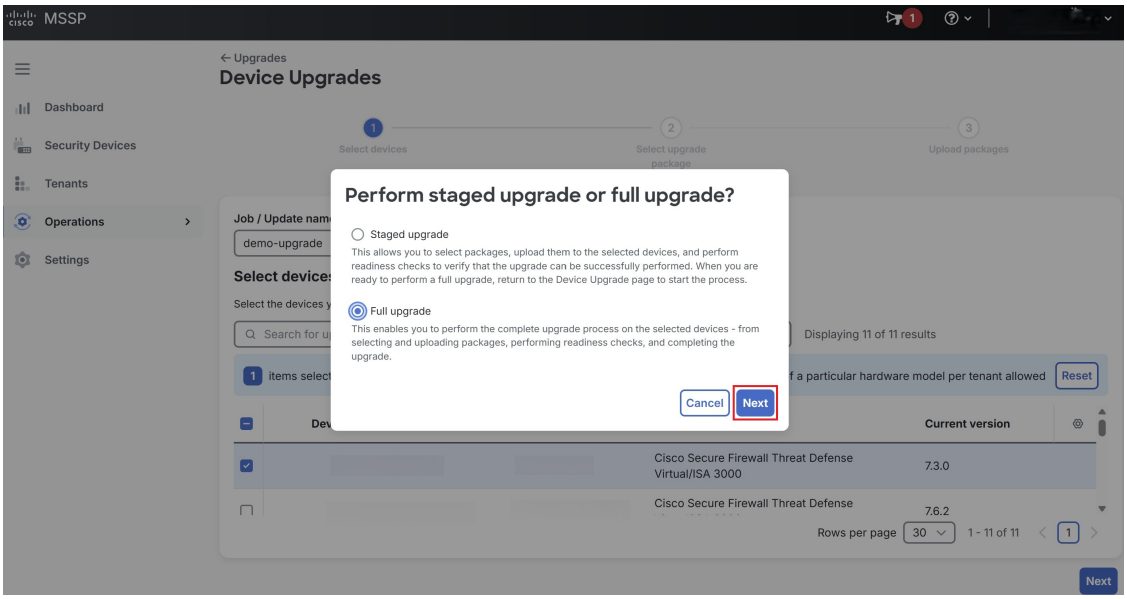
ステップ 2 [Begin an Upgrade] をクリックします。

ステップ 3 アップグレードの名前を入力し、アップグレードするデバイスを選択して、**[Next]** をクリックします。

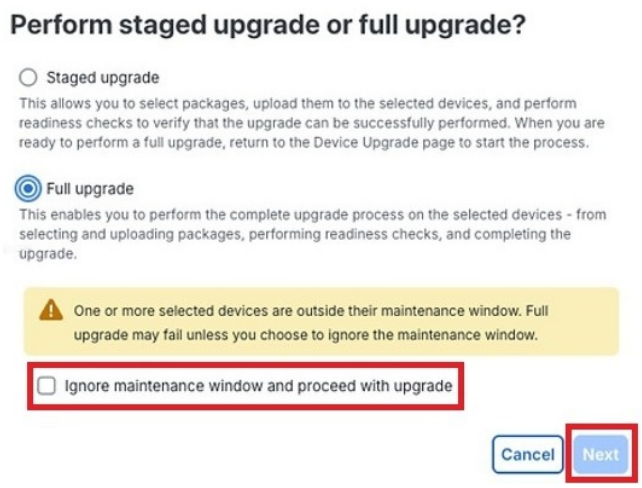
[デバイスのアップグレード（Device Upgrades）] ページの上部にある **[モデル（Model）]** または **[テナント（Tenant）]** ドロップダウンリストを使用して、デバイスをフィルタ処理します。

（注）
特定のハードウェアモデルに属する最大 50 台のデバイスを各テナントに対してアップグレードできます。

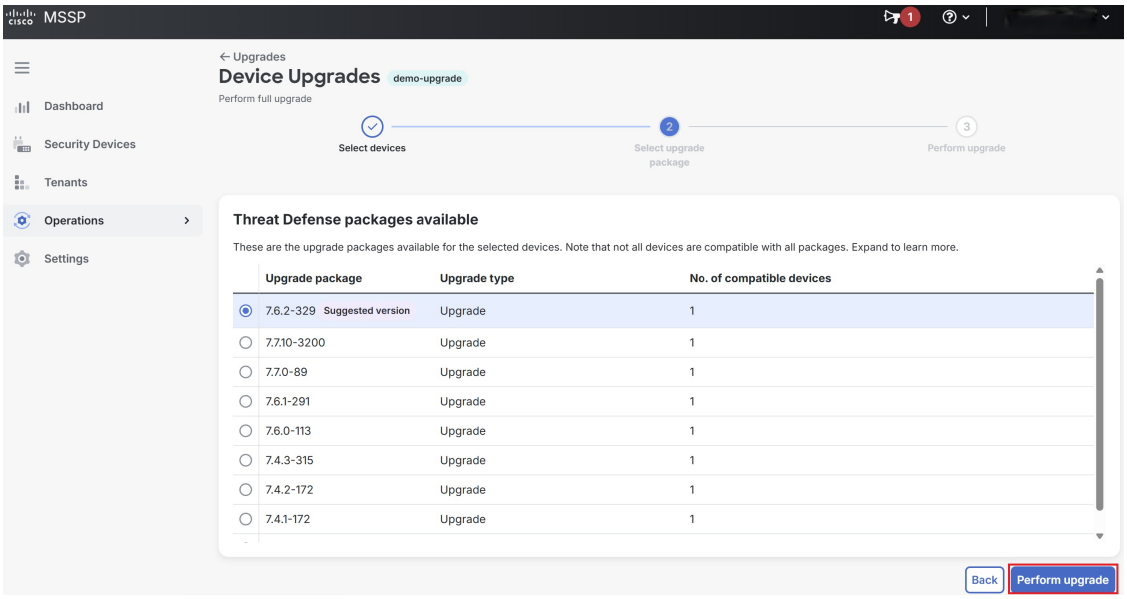
ステップ 4 表示されるダイアログボックスで **[Full upgrade]** ボタンをクリックし、**[Next]** をクリックします。



メンテナンスウィンドウ外にあるデバイスでフルアップグレードを実行するには、**[Ignore maintenance window and proceed with upgrade]** をクリックしてから、**[Next]** をクリックします。メンテナンスウィンドウ外でアップグレードを実行することは推奨されていません。緊急の場合にのみ実行してください。



ステップ 5 選択したデバイスで**使用可能な Threat Defense パッケージ**のリストからアップグレードパッケージを選択し、**[Perform upgrade]** をクリックします。すべてのデバイスがすべてのパッケージと互換性があるわけではないことに注意してください。



ステップ 6 **[Back to Upgrades]** をクリックして、**[Upgrades]** ページに戻ります。

アップグレードが完了すると、**[Upgrades]** ページの **[Status]** 列の下に、**[Upgrade completed]** というメッセージが表示されます。アップグレードが失敗すると、失敗の理由を示すメッセージが表示されます。

MSSP ポータルでのステージングされたマルチテナントデバイスのアップグレードの開始

段階的なアップグレードを開始する場合は、パッケージを選択して選択したデバイスにアップロードし、準備状況チェックを実行します。これらのチェックは、後でアップグレードを正常に実行できることを確認します。

ヒント ステージングアップグレードを使用して、メンテナンスウィンドウの前にアップグレードの準備を行うことができます。これにより、実際のアップグレードウィンドウでフルアップグレードをより迅速に完了できます。

段階的なアップグレードを開始するには、次の手順を実行します。

手順

ステップ 1 左側のペインから、**[Operations]** > **[Upgrades]** に移動します。

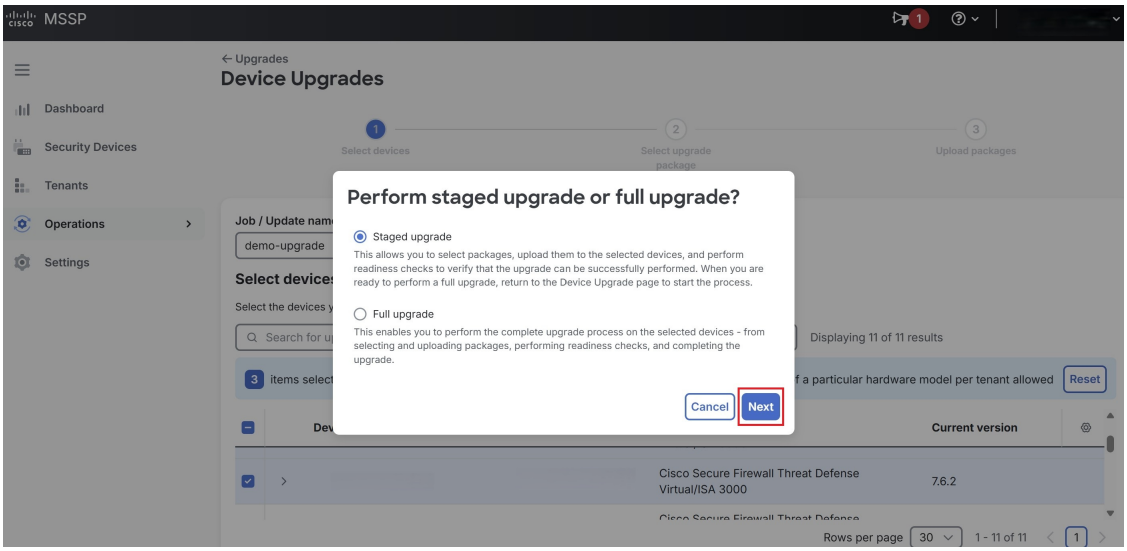
ステップ 2 [Begin Upgrade] をクリックします。

ステップ 3 アップグレードの名前を入力し、アップグレードするデバイスを選択して、**[Next]** をクリックします。

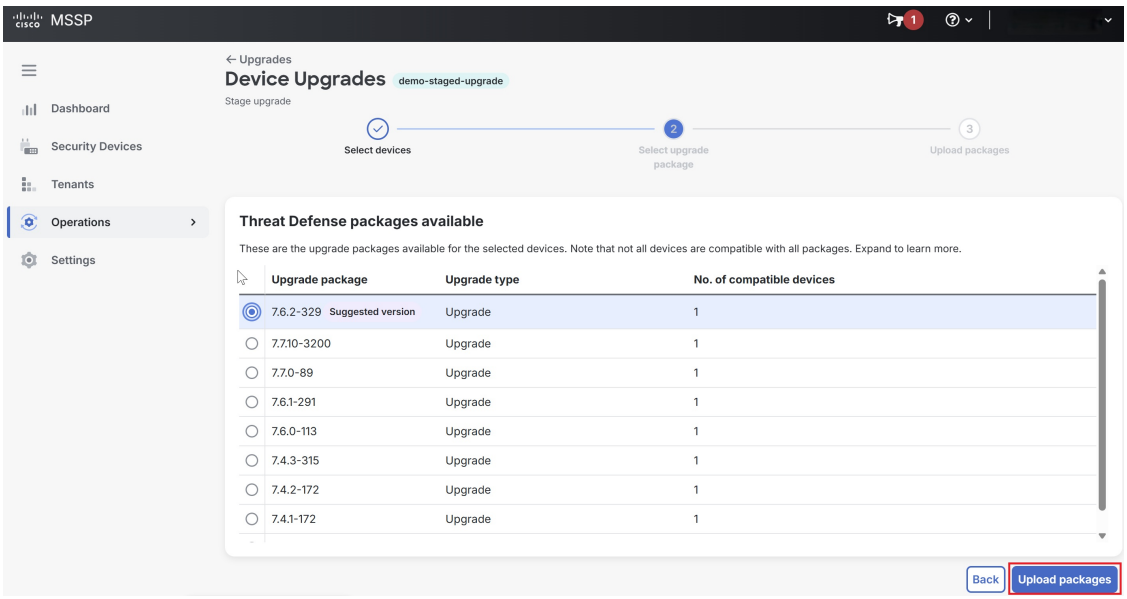
[Device Upgrades] ページの上部にある **[Model]** または **[Tenant]** ドロップダウンリストを使用して、デバイスをフィルタ処理します。

（注）
特定のハードウェアモデルに属する最大 50 台のデバイスを各テナントに対してアップグレードできます。

ステップ 4 表示されるダイアログボックスで **[Staged upgrade]** ボタンをクリックし、**[Next]** をクリックします。



ステップ 5 選択したデバイスで使用可能な Threat Defense パッケージのリストからアップグレードパッケージを選択し、**[Upload packages]** をクリックします。すべてのデバイスがすべてのパッケージと互換性があるわけではないことに注意してください。



ステップ 6 アップロードを取り消すには、**[Exit]** をクリックします。

パッケージがアップロードされると、**[Upgrades]** ページの **[Status]** 列の下に「**アップグレードパッケージがアップロードされ、ステージングされました**」というメッセージが表示されます。

ステップ 7 [終了（Exit）] をクリックします。

アップグレードパッケージがステージングされ、インストールする準備が整っています。**[Upgrade staged]**ステータスは、**[Upgrades]** ページの **[Status]** 列で確認できます。準備ができたら、**[Upgrades]** ページの **[Upgrade name]** 列でアップグレード名をクリックして、フルアップグレードを続行します。

MSSP ポータルの [Security Devices] ページから一括アップグレードを実行

[Security Devices] ページからデバイスを直接アップグレードするには、この手順を使用します。

手順

ステップ 1 左側のペインで、[セキュリティデバイス（Security Devices）] をクリックします。

ステップ 2 アップグレードするデバイスを選択し、右側にある **[Actions]** で **[Upgrade device]** をクリックします。

選択したデバイスが **[Device Upgrades]** ページにリダイレクトされます。

ステップ 3 アップグレードの名前を入力し、**[Device Upgrade]** ダイアログボックスで **[Staged upgrade]** または **[Full upgrade]** を選択し、**[Next]**をクリックします。

[Full upgrade]を選択した場合は、MSSP ポータルでのマルチテナントデバイスのフルアップグレードの開始 （34 ページ） のステップ 4 からステップ 7 を実行します。

[Staged upgrade]を選択した場合は、MSSP ポータルでのステージングされたマルチテナントデバイスのアップグレードの開始 （36 ページ） のステップ 4 からステップ 7 を実行します。

MSSP ポータル設定の管理

Security Cloud Control では、設定ページで MSSP ポータルと個人ユーザーアカウントの特定の部分をカスタマイズできます。左側のペインの [Settings] をクリックして、設定ページにアクセスします。

設定

全般設定

Cisco ASA のヘルスモニタリング機能を有効にすると、**[Health overview]** ダッシュボードを使用して MSSP ポータルで Secure Firewall Cisco ASA デバイスをモニターできます。

また、**[General Settings]**で**ポータル ID**、**Cisco Secure Services Exchange ポータル ID** 、および**ポータル名**を表示することもできます。

ユーザー 管理

MSSP ポータルに関連付けられているすべての**ユーザー**、 **Active Directoryグループ**、および**監査ログを [User Management]** 画面で表示できます。

左側のペインで、[Settings]> [**User Management**] の順にクリックします。

1. **ユーザー（Users）**：**[Users]** タブで、テナントに関連付けられたすべてのユーザーレコードを表示できます。

   - **[Users]** タブで、**[Generate API Token]** をクリックして、API 専用ユーザーのための API トークンを生成します。

     機密データを取り扱うための企業のベストプラクティスに従って、トークンを安全な場所に保存します。詳細については、API トークンの生成 （21 ページ）を参照してください。

   - API トークンを更新するには、**[Token]** 列の下の **[Refresh]** をクリックします。詳細については、API トークンの更新 （22 ページ）を参照してください。

   - API トークンを取り消すには、**[Token]** 列の下の **[Revoke]** をクリックします。詳細については、API トークンの取り消し （23 ページ）を参照してください。

2. **Active Directory グループ（Active Directory Groups）**：転換率が高いテナントの場合、MSSP ポータルを Active Directory グループにマッピングすることで、個々のユーザーを MSSP ポータルに追加する代わりに、ユーザーリストとロールを簡単に管理できます。新しいユーザーの追加や既存のユーザーの削除といったユーザーの変更はすべて、Active Directory で実行できるようになり、MSSP で実行する必要がなくなります。

   - [Active Directory グループ（Active Directory Groups）] タブをクリックします。このページには、Active Directory マネージャで割り当てられた Active Directory グループのロールが表示されます。

     詳細については、ユーザー管理の Active Directory グループ （42 ページ）を参照してください。

3. **監査ログ（Audit Logs）**：**[Audit Logs]** 機能は、MSSP ポータルでユーザー関連およびシステムレベルのアクションを記録します。

   - [監査ログ（Audit Logs）] タブをクリックします。

     現在のテナントのイベントとアクティビティのリストが表示されます。

特定のユーザーのログを検索するには、[検索（Search）] テキストボックスを使用します。

- フィルタアイコンをクリックして、検索結果を絞り込み、特定のイベントを表示します。

  [時間範囲（Time Range）] と [イベントアクション（Event Action）] に基づいてログをフィルタ処理できます。

- **[Export]**をクリックして、詳細を CSV 形式でダウンロードします。

スイッチテナント

複数のポータルテナントがある場合、Security Cloud Control からサインアウトせずに、異なるポータルまたはテナント間で切り替えることができます。

手順

ステップ 1 MSSP ポータルで、右上隅に表示されるテナントメニューをクリックします。
ステップ 2 [Switch tenant] をクリックします。
ステップ 3 表示するポータルまたはテナントを選択します。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウドサービスです。Cisco Success Network を有効にすると、デバイスと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、デバイスからの対象のデータを選択してそれを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカル サポート サービスとモニターリングについて通知します。
- シスコ製品の改善に役立ちます。

デバイスは常にセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。デバイスを登録した後で Cisco Success Network の設定を変更できます。

（注）

- Firewall Threat Defense ハイアベイラビリティペアでは、アクティブデバイスを選択すると、スタンバイデバイスの Cisco Success Network 設定を上書きします。
- Security Cloud Control は Cisco Success Network 設定を管理しません。設定の管理とテレメトリ情報の提供は、Firewall Device Manager ユーザーインターフェイスが行います。

Cisco Success Network の有効化または無効化

システムの初期設定時に、Cisco Smart Software Manager にデバイスを登録するように求められます。登録せずに 90 日間の評価ライセンスを使用する場合、評価期間の終了前にデバイスを登録する必要があります。デバイスを登録するには、（[スマートライセンス（Smart Licensing）] ページで）Cisco Smart Software Manager にデバイスを登録するか、または登録キーを入力して Security Cloud Control に登録します。

デバイスを登録すると、バーチャル アカウントからデバイスにライセンスが割り当てられます。デバイスを登録すると、有効にしているすべてのオプション ライセンスも登録されます。

この接続は、Cisco Success Network を無効にすることでいつでも無効にできますが、このオプションは Firewall Device Manager UI からのみ無効にできます。無効にすると、デバイスがクラウドから切断されます。切断しても更新の受信やスマート ライセンス機能の操作には影響せず、正常に動作を継続します。詳細については、『Firepower Device Manager コンフィギュレーション ガイド、バージョン 6.4.0 以降』の「システム管理」の章の「**Cisco Success Network への接続**」セクションを参照してください。

Security Cloud Control でのユーザーの管理

Security Cloud Control でユーザーレコードを作成または編集する前に、「アイデンティティ プロバイダー アカウントと Security Cloud Control ユーザーレコードとの関係」を読んで、ID プロバイダー（IdP）アカウントとユーザーレコードがどのように相互作用するかを学習してください。Security Cloud Control ユーザーは、認証されて Security Cloud Control テナントにアクセスできるように、レコードと対応する IdP アカウントが必要です。

企業独自の IdP がない限り、Cisco Secure Sign-On はすべての Security Cloud Control テナントの ID プロバイダーとなります。この記事の残りの部分は、ID プロバイダーとして Cisco Secure Sign-On を使用していることを前提としています。

テナントに関連付けられているすべてのユーザーレコードは、**ユーザー管理**画面で確認できます。サポートチケットを解決するために一時的にアカウントに関連付けられたシスコサポートエンジニアも対象となります。

テナントのネットワーク管理者の管理

テナントのネットワーク管理者の数を制限することを、ベストプラクティスとしてお勧めします。ネットワーク管理者権限を持つユーザーを決定し、[ユーザー管理（User Management）] を確認して、他のユーザーの役割を「管理者」に変更します。

テナントに関連付けられている API ユーザーレコードの表示

手順

ステップ 1 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 2 左側のペインで **Administration** > **API User Management** をクリックします。

ユーザー管理の Active Directory グループ

多数のユーザーが頻繁に入れ替わるテナントの場合、個々のユーザーを Security Cloud Control に追加する代わりに、Security Cloud Control を Active Directory（AD）グループにマッピングして、ユーザーリストとユーザーロールをより簡単に管理できます。新しいユーザーの追加や既存のユーザーの削除といったユーザーの変更はすべて、Active Directory で実行できるようになり、Security Cloud Control で実行する必要がなくなります。

[ユーザー管理（User Management）] ページから Active Directory グループを追加、編集、または削除するには、[ネットワーク管理者（SuperAdmin）] ユーザーロールが必要です。詳細については、「ユーザーロール」を参照してください。

左側のペインで、[設定（Settings）]>[ユーザー管理（User Management）] の順に選択します。

Active Directory グループ

- 左側のペインで、[**Administration** > **API User Management**] > [Active Directoryグループ（Active Directory Groups）] をクリックします。
- このページには、Active Directory マネージャで割り当てられた Active Directory グループのロールが表示されます。
- Active Directory グループに含まれているユーザーは、[Active Directoryグループ（Active Directory Groups）] タブまたは [ユーザー（Users）] タブに個別に表示されません。

監査ログ

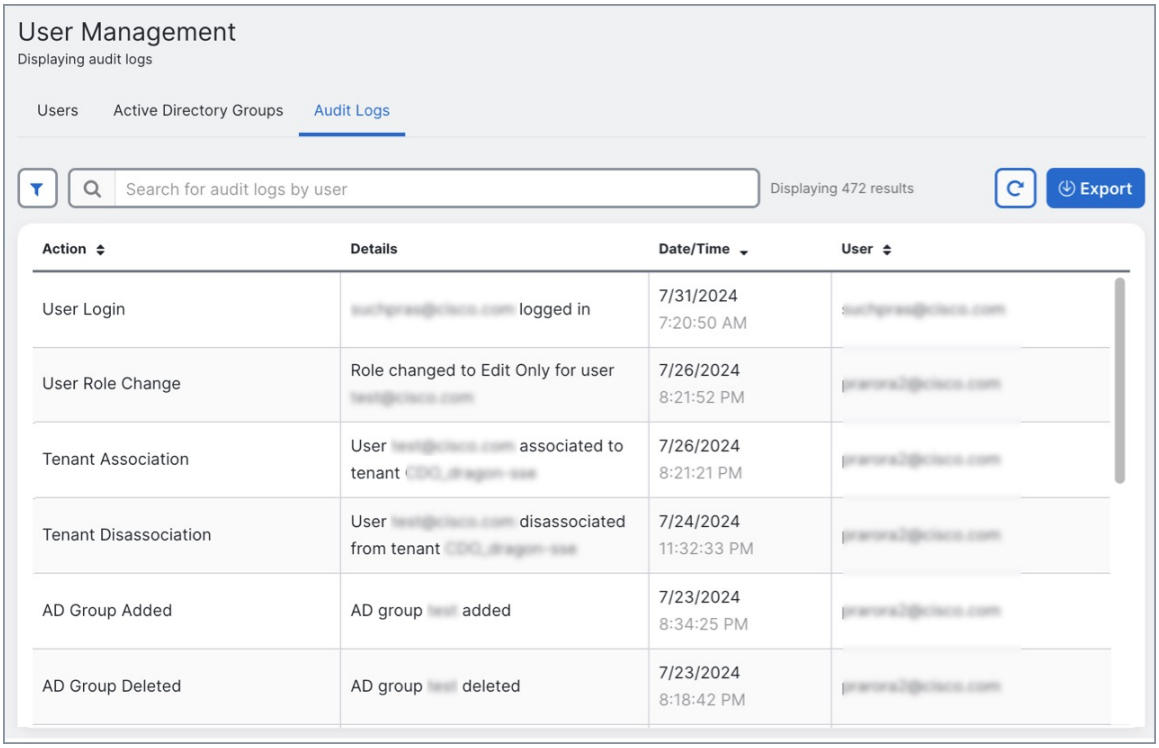
Security Cloud Control の [監査ログ（Audit Logs）] には、ユーザー関連およびシステムレベルのアクションが記録されます。[監査ログ（Audit Logs）] によってキャプチャされる主なイベントは次のとおりです。

- **ユーザーログイン**：ユーザー認証のすべてのインスタンスを記録します。
- **テナントの関連付けと関連付け解除**：テナントとのユーザーの関連付けまたは関連付け解除を追跡します。
- **ユーザーロールの変更**：ユーザーロールの変更を記録します。
- **Active Directory グループ**：AD グループ内の追加、削除、およびロールの変更を記録します。

手順：

1. 左側のペインで **Administration** > **API User Management** をクリックします。
2. [監査ログ（Audit Logs）] タブをクリックします。現在ログイン中のテナントのイベントとアクティビティのリストが表示されます。
3. 特定のユーザーのログを検索するには、[検索（Search）] テキストボックスを使用します。
4. フィルタアイコンをクリックして、検索結果を絞り込み、特定のイベントを表示します。[時間範囲（Time Range）] と [イベントアクション（Event Action）] に基づいてログをフィルタ処理できます。
5. [エクスポート（Export）] をクリックして、詳細を CSV 形式でダウンロードします。

図 *1* : 監査ログ



マルチロールユーザー

Security Cloud Control の IAM 機能が拡張され、ユーザーが複数のロールを持つことができるようになりました。

ユーザーは Active Directory の複数のグループに属している場合があり、それらのグループは、Security Cloud Control において異なる Security Cloud Control ロールで定義できます。ユーザーがログイン時に取得する最終的な権限は、そのユーザーが属している、Security Cloud Control で定義されているすべての Active Directory グループのロールの組み合わせです。たとえば、ユーザーが 2 つの Active Directory グループに属しており、両方のグループが 2 つの異なるロール（編集専用とデプロイ専用など）で Security Cloud Control に追加されている場合、ユーザーは編集専用とデプロイ専用の両方の権限を持ちます。これは、任意の数のグループとロールに適用されます。

Active Directory グループのマッピングを Security Cloud Control で定義する必要があるのは 1 回だけであり、ユーザーのアクセスと権限の管理は、その後、異なるグループ間でユーザーを追加、削除、または移動することによって Active Directory で排他的に実行できます。

（注） ユーザーが、個人ユーザーであり、かつ同じテナントの Active Directory グループにも属している場合は、個人ユーザーのユーザーロールが Active Directory グループのユーザーロールよりも優先されます。

Active Directory グループ用 API エンドポイント

ネットワーク管理者は、API エンドポイントを使用して次の操作を実行できます。

- Active Directory グループの作成
- Active Directory グループの削除
- Active Directory グループの変更
- Active Directory グループの取得
- Active Directory グループの取得

前述のリンクで、Cisco DevNet Web サイトの対応するセクションに移動できます。

Active Directory グループを Security Cloud Control に追加するための前提条件

ユーザー管理の一種として Active Directory グループマッピングを Security Cloud Control に追加するには、まず Security Cloud Sign On に統合済みの Active Directory が必要です。Active Directory ID プロバイダー（IdP）がまだ統合されていない場合は、「Identity provider integration guide」[英語] を参照して、カスタム Active Directory IdP 統合に次の情報を統合します。

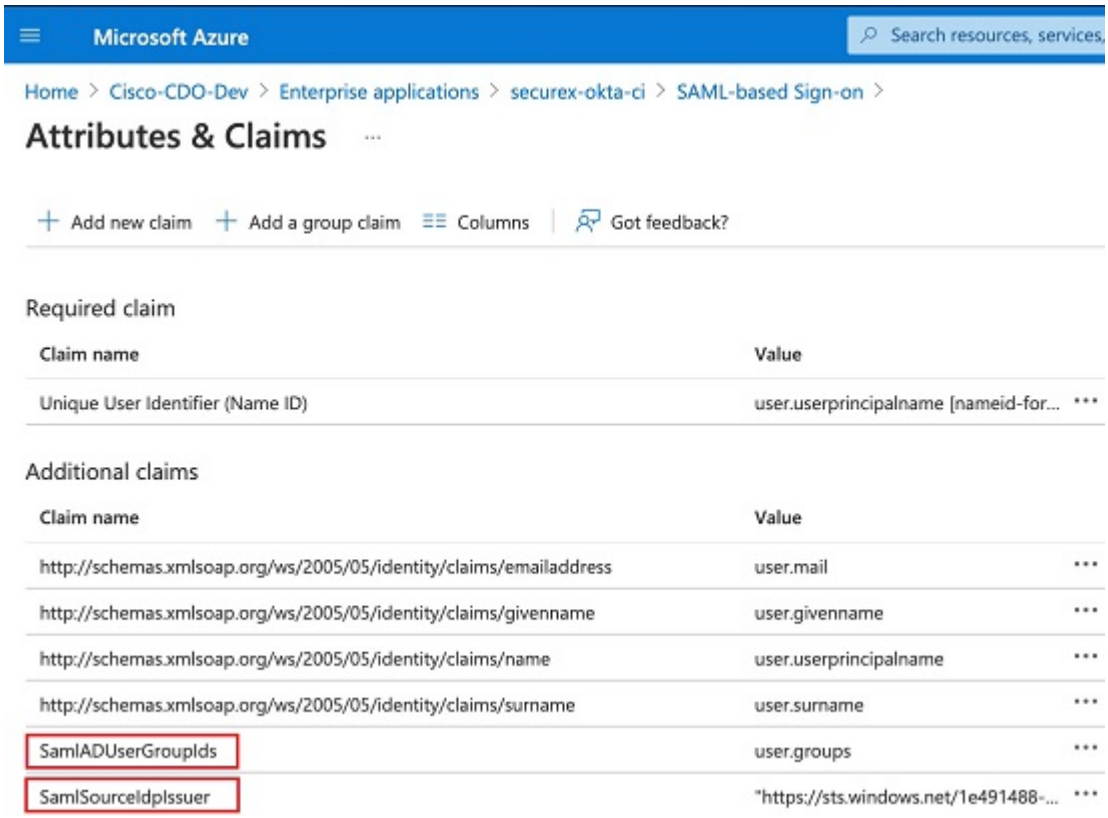
- Security Cloud Control のテナント名とリージョン

- カスタムルーティングを定義するドメイン（例：@cisco.com、@myenterprise.com）
- XML 形式の証明書とフェデレーションメタデータ

Active Directory の統合が完了したら、Active Directory に次のカスタム SAML 要求を追加します。Active Directory の統合が完了した後に Security Cloud Control テナントにサインインするには、SAML 要求と属性が必要です。これらの値では大文字と小文字が区別されます。

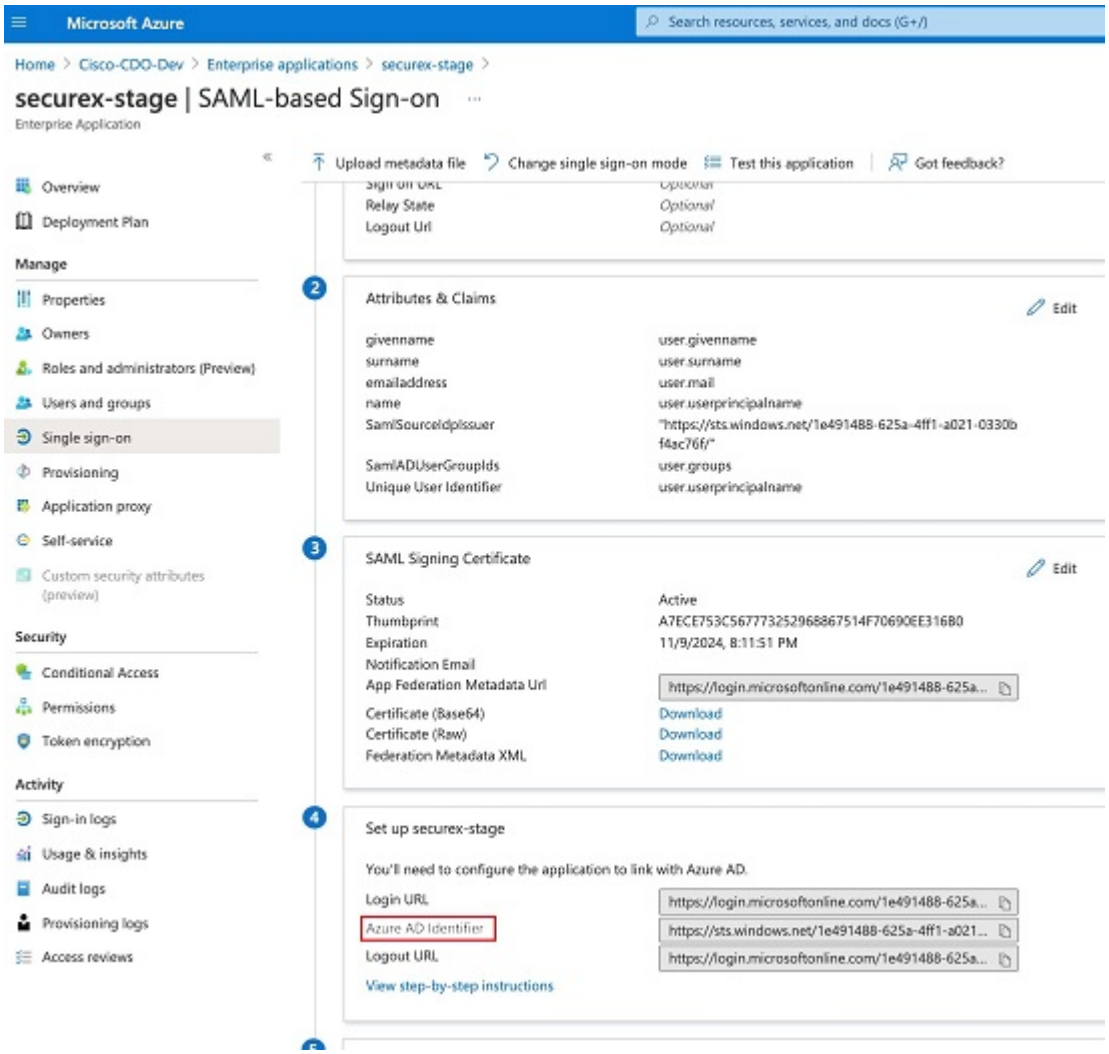
- **SamlADUserGroupIds**：この属性は、ユーザーが Active Directory 上で持つすべてのグループの関連付けを記述します。たとえば、次のスクリーンショットに示すように、Azure で [+グループ要求の追加（+ Add groups claim）] を選択します。

図 *2 : Active Directory* で定義されたカスタム要求



- **SamlSourceIdpIssuer**：この属性は、Active Directory インスタンスを一意に識別します。たとえば、次のスクリーンショットに示すように、Azure で [+グループ要求の追加（+ Add a group claim）] を選択し、スクロールして Azure Active Directory 識別子を見つけます。

図 *3 : Azure Active Directory* の識別子を見つける



ユーザー管理用 Active Directory グループの追加

Active Directory グループを追加、編集、または削除するには、[ネットワーク管理者（SuperAdmin）] ユーザーロールが必要です。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 [Active Directory グループ（Active Directory Groups）] タブをクリックします。

ステップ 5 Active Directory グループの追加（  ）ボタンをクリックします。

ステップ 6 次の情報を入力します。

- [グループ名（Group Name）]：一意の名前を入力します。この名前は、Active Directory のグループ名と一致する必要はありません。Security Cloud Control は、このフィールドの特殊文字をサポートしていません。
- [グループID（Group Identifier）]：Active Directory からグループ ID を手動で入力します。グループ ID の値は、カスタム要求定義のグループ ID と同じである必要があります。この値は、グループの一意の ID に対応する任意の値（my-favourite-group、12345 など）にすることができます。
- [AD発行者（AD Issuer）]：Active Directory から Active Directory の発行者の値を手動で入力します。
- [ロール（Role）]：ユーザーロールを選択します。この Active Directory グループに含まれるすべてのユーザーのロールが決まります。詳細については、「ユーザーロール」を参照してください。
- （オプション）[注記（Notes）]：この Active Directory グループに適用される注記を追加します。

ステップ 7 **[OK]** を選択します。

ユーザー管理用 Active Directory グループの編集

始める前に

Security Cloud Control で Active Directory グループのユーザー管理を編集する場合は、Security Cloud Control が Active Directory グループを制限する方法だけを変更できることに注意してください。Security Cloud Control で Active Directory グループそのものの編集はできません。Active Directory グループ内のユーザーリストを編集するには、Active Directory を使用する必要があります。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 [Active Directory グループ（Active Directory Groups）] タブをクリックします。

ステップ 5 編集する Active Directory グループを特定し、編集アイコンをクリックします。

ステップ 6 次の値を変更します。

- [グループ名（Group Name）]：一意の名前を入力します。Security Cloud Control は、このフィールドの特殊文字をサポートしていません。
- [グループID（Group Identifier）]：Active Directory からグループ ID を手動で入力します。グループ ID の値は、カスタム要求定義のグループ ID と同じである必要があります。この値は、グループの一意の ID に対応する任意の値（my-favourite-group、12345 など）にすることができます。
- [AD発行者（AD Issuer）]：Active Directory から Active Directory の発行者の値を手動で入力します。
- [ロール（Role）]：この Active Directory グループに含まれるすべてのユーザーのロールが決まります。詳細については、「ユーザーロール」を参照してください。
- [注記（Notes）]：この Active Directory グループに適用される注記を追加します。

ステップ 7 [OK] をクリックします。

ユーザー管理用 Active Directory グループの削除

手順

ステップ 1 Security Cloud Control にログインします。
ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。
ステップ 4 [Active Directory グループ（Active Directory Groups）] タブをクリックします。
ステップ 5 削除する Active Directory グループを指定します。
ステップ 6 [Delete] アイコンをクリックします。
ステップ 7 [OK] をクリックして、Active Directory グループを削除することを確認します。

Security Cloud Control の新規ユーザーの作成

Security Cloud Control ユーザーの新規作成では、次の 2 つのタスクが必要です。次の順序で実行する必要はありません。

- 新規ユーザー向け Cisco Secure Sign-On アカウントの作成
- Security Cloud Control ユーザー名による Security Cloud Control ユーザーレコードの作成

これらのタスクが完了すると、ユーザーは Cisco Secure Sign-On ダッシュボードから Security Cloud Control を開くことができます。

新規ユーザー向け Cisco Security Cloud Sign On アカウントの作成

新規ユーザーは、割り当て先のテナント名を知らなくても、いつでも Cisco Security Cloud Sign On アカウントを作成できます。

Security Cloud Control へのログインについて

Security Cloud Control は、Cisco Secure Sign-On を アイデンティティ プロバイダーとして使用し、Duo を多要素認証（MFA）に使用します。**Security Cloud Control にログインするには、まず Cisco Security Cloud Sign On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。**

Security Cloud Control には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、Security Cloud Control にログインするユーザーの ID を確認するために、2 つのコンポーネントまたは要素が必要です。最初の要素はユーザー名とパスワードで、2 番目の要素はオンデマンドで生成されるワンタイムパスワード（OTP）です。

ログインする前に

Duo Security のインストール

Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。

時刻の同期

モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが自動的に、または手動で正しい時刻に設定されていることを確認します。

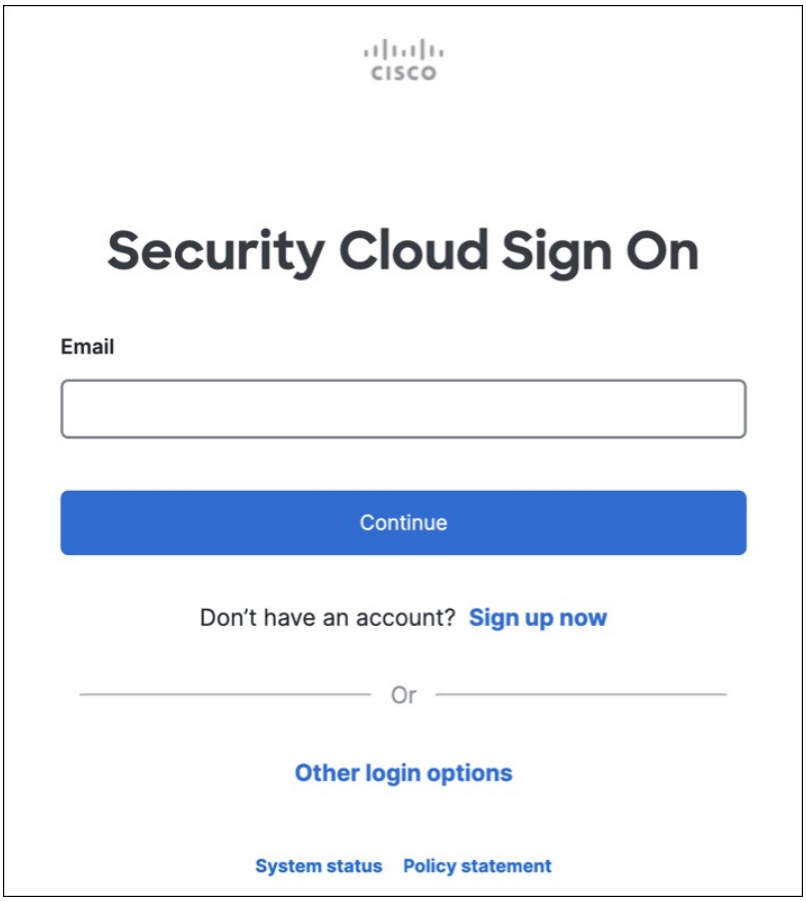
新規 Cisco Security Cloud Sign On アカウントの作成と Duo 多要素認証の設定

最初のサインオンワークフローは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

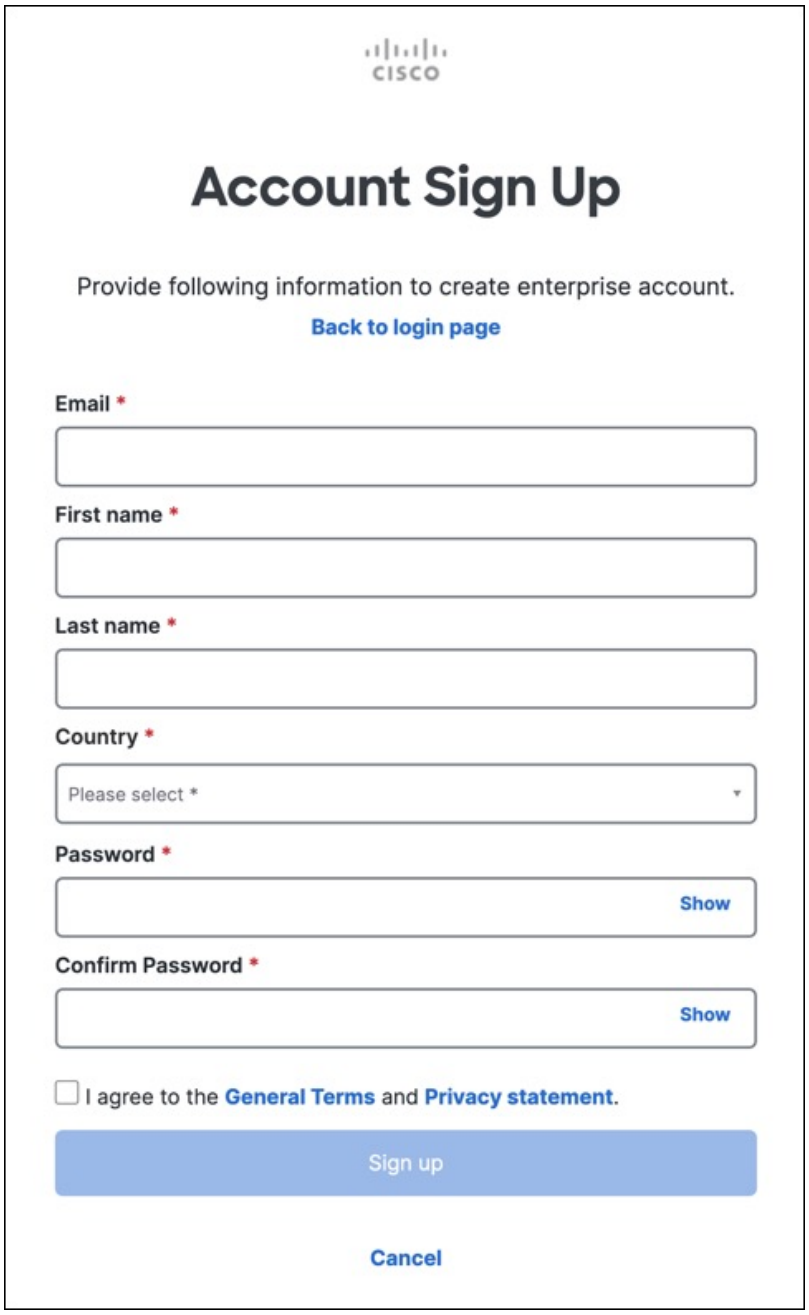
手順

ステップ 1　新しい Cisco Security Cloud Sign On アカウントにサインアップします。

1. https://security.cisco.com を開きます。
2. サインイン画面の下部にある [今すぐサインアップ（Sign up now）] をクリックします。



3. エンタープライズアカウントを作成するには、次の情報を入力します。



次にいくつかのヒントを示します。

- [電子メール（Email）]：Security Cloud Control へのログインに最終的に使用する電子メールアドレスを入力します。
- [パスワード（Password）]：強力なパスワードを入力します。

4. [サインイン（Sign up）] をクリックします。

その後、登録したアドレスに確認メールが送信されます。電子メールを開き、[アカウントの有効化（Activate account）] をクリックします。

ステップ 2　Duo を使用して多要素認証をセットアップする

多要素認証をセットアップするときは、モバイルデバイスを使用することをお勧めします。

1. [多要素認証の設定（Set up multi-factor authentication）] 画面で、[要素の設定（Configure factor）] をクリックします。
2. [セットアップの開始（Start setup）] をクリックし、プロンプトに従ってモバイルデバイスを選択して、そのモバイルデバイスとアカウントのペアリングを確認します。

   詳細については、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。デバイスにDuoアプリケーションがすでにインストールされている場合は、このアカウントのアクティベーションコードが送信されます。Duo は 1 台のデバイスで複数のアカウントをサポートします。
3. ウィザードの最後で、[ログインを続行する（Continue to Login）] をクリックします。
4. 二要素認証を使用して Cisco Security Cloud Sign On にログインします。

ステップ 3　（任意）追加のオーセンティケータとして Google オーセンティケータを設定します。

1. Googleオーセンティケータとペアリングするモバイルデバイスを選択し、[次へ（Next）] をクリックします。
2. セットアップウィザードのプロンプトに従って、Googleオーセンティケータをセットアップします。

ステップ 4　Cisco Security Cloud Sign On のアカウントリカバリのオプションを設定する

1. SMS を使用してアカウントをリセットするための予備の電話番号を選択します。
2. セキュリティイメージを選択します。
3. [マイアカウントの作成（Create My Account）] をクリックします。

Security Cloud Control ユーザー名でのユーザーレコードの作成

「ネットワーク管理者（Super Admin）」権限を持つ Security Cloud Control ユーザーのみが Security Cloud Control ユーザーレコードを作成できます。「ネットワーク管理者」は、上記の **Security Cloud Control ユーザー名の作成**タスクで指定したものと同じ電子メールアドレスでユーザーレコードを作成する必要があります。

次の手順を使用して、適切なユーザーロールを持つユーザーレコードを作成します。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで、[設定（Settings）]>[ユーザー管理（User Management）] の順に選択します。

ステップ 4  をクリックして、新しいユーザーをテナントに追加します。

ステップ 5 ユーザーの電子メールアドレスを入力します。

（注）
ユーザーの電子メールアドレスは、Cisco Secure Log-On アカウントの電子メールアドレスに対応している必要があります。

ステップ 6 [ロール（Role）] ドロップダウンリストから、ユーザーのロールを選択します。

ステップ 7 [OK] をクリックします。

新規ユーザーが Cisco Secure Sign-On ダッシュボードから Security Cloud Control を開く

手順

ステップ 1 Cisco Secure Sign-on ダッシュボードで、テナントのリージョンに適した [Security Cloud Control] タイルをクリックします。

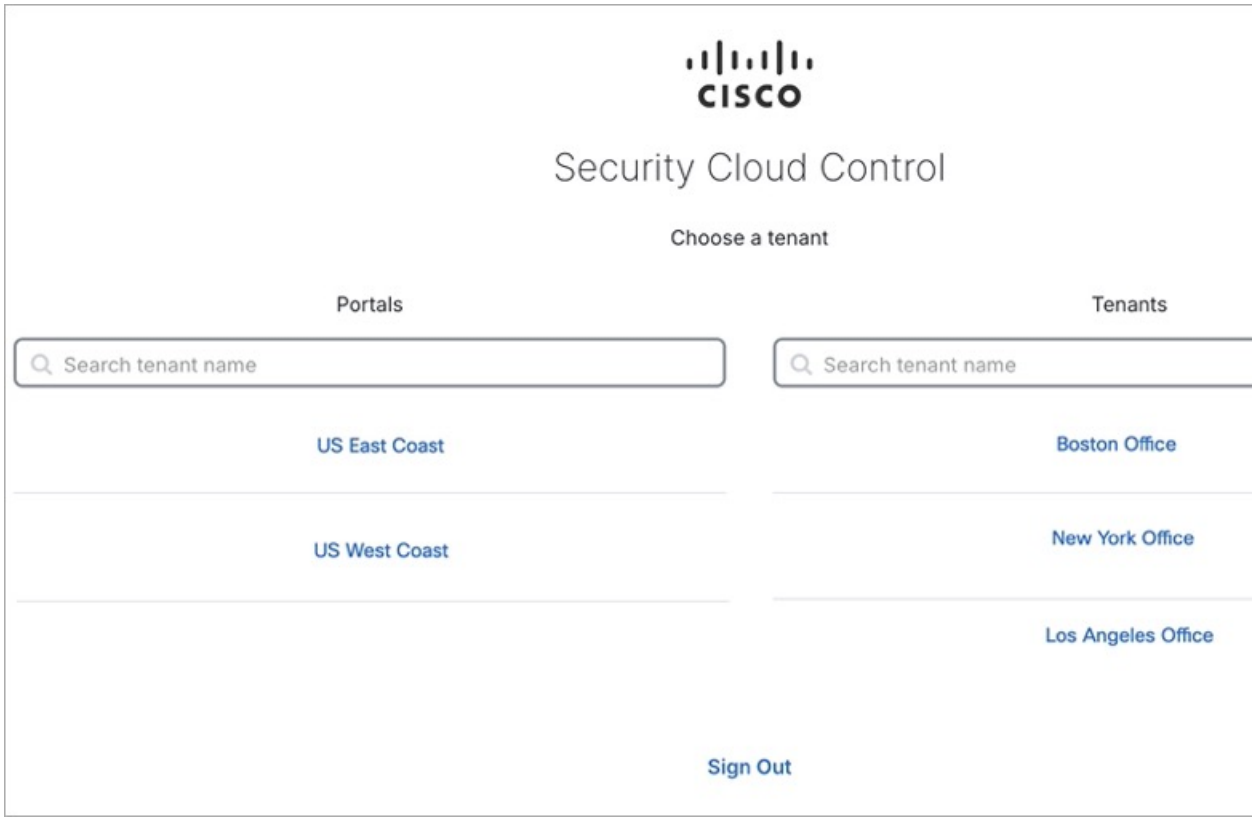
ステップ 2 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザーレコードがある場合は、そのテナントにログインします。
- 複数のポータルにすでにユーザーレコードがある場合は、接続するポータルを選択できます。
- すでに複数のテナントにユーザーレコードがある場合は、接続先の Security Cloud Control テナントを選択できます。
- 既存のテナントにユーザーレコードがない場合は、Security Cloud Control の詳細を確認するか、またはトライアルテナントを要求できます。

[ポータル（Portals）] ビューは、複数のテナントから統合された情報を取得して表示します。

詳細については、「複数の Security Cloud Control テナントの管理」を参照してください。

[テナント（Tenant）] ビューには、ユーザーレコードがある一部のテナントが表示されます。



Security Cloud Control のユーザーロール

Security Cloud Control には、読み取り専用、編集専用、展開専用、管理者、ネットワーク管理者など、さまざまなユーザーロールがあります。ユーザーロールは、各テナントのユーザーごとに設定されます。1 人の Security Cloud Control ユーザーが複数のテナントにアクセスできる場合、ユーザーIDは同じでも、テナントごとにロールが異なる場合があります。ユーザーは、あるテナントで読み取り専用ロールを持ち、別のテナントでネットワーク管理者ロールを持つ場合があります。インターフェイスまたはマニュアルで読み取り専用ユーザー、管理者ユーザー、ネットワーク管理者ユーザーについて言及されている場合、特定のテナントにおけるそのユーザーの権限レベルが説明されています。

読み取り専用ロール

読み取り専用ロールが割り当てられたユーザーには、すべてのページに次の青いバナーが表示されます。

Read Only User. You cannot make configuration changes.

読み取り専用ロールを持つユーザーは、次のことを実行できます。

- Security Cloud Control の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。読み取り専用ユーザーは、自分のトークンを取り消すと、再作成できないことに注意してください。
- インターフェイスからサポートに連絡し、変更ログをエクスポートする。

読み取り専用ユーザーは、次のことを実行**できません**。

- 任意のページで作成、更新、設定、または削除する。
- デバイスをオンボーディングする。
- オブジェクトやポリシーなどの作成に必要なタスクのステップスルーはできるが保存はできない。
- Security Cloud Control ユーザーレコードを作成する。
- ユーザーロールを変更する。
- アクセスルールをポリシーにアタッチまたはデタッチする。

編集専用ロール

編集専用ロールを持つユーザーは、次の操作を実行できます。

- オブジェクト、ポリシー、ルールセット、インターフェース、VPNなどを含むがこれらに限定されないデバイス構成を編集および保存する。
- **構成の読み取り**アクションによって行われた構成の変更を許可する。
- 変更リクエスト管理アクションを利用する。

編集専用ユーザーは、次の操作を実行**できません**。

- 1 つまたは複数のデバイスに変更を展開する。
- 段階的な変更または OOB によって検出された変更を破棄する。
- AnyConnect パッケージをアップロードする、またはこれらの設定を構成する。
- デバイスのイメージアップグレードをスケジュールする、または手動で開始する。
- セキュリティデータベースのアップグレードをスケジュールする、または手動で開始する。

- Snort 2 と Snort 3 のバージョンを手動で切り替える。
- テンプレートを作成します。
- 既存の OOB 変更の設定を変更する。
- システム管理設定を編集する。
- デバイスをオンボーディングする。
- デバイスを削除する。
- VPN セッションまたはユーザーセッションを削除する。
- Security Cloud Control ユーザーレコードを作成する。
- ユーザーロールを変更する。

展開専用ロール

展開専用ロールを持つユーザーは、次の操作を実行できます。

- 段階的な変更を単一のデバイスまたは複数のデバイスに展開する。
- ASA デバイスの設定変更を元に戻すか、復元する。
- デバイスのイメージアップグレードをスケジュールする、または手動で開始する。
- セキュリティデータベースのアップグレードをスケジュールする、または手動で開始する。
- 変更要求管理アクションを使用する。

展開専用ユーザーは、次の操作を実行**できません**。

- Snort 2 と Snort 3 のバージョンを手動で切り替える。
- テンプレートを作成します。
- 既存の OOB 変更の設定を変更する。
- システム管理設定を編集する。
- デバイスをオンボーディングする。
- デバイスを削除する。
- VPN セッションまたはユーザーセッションを削除する。
- 任意のページで作成、更新、設定、または削除する。
- デバイスをオンボーディングする。
- オブジェクトやポリシーなどの作成に必要なタスクのステップスルーはできるが保存はできない。

- Security Cloud Control ユーザーレコードを作成する。
- ユーザーロールを変更する。
- アクセスルールをポリシーにアタッチまたはデタッチする。

VPN セッションマネージャロール

VPN セッションマネージャロールは、サイト間 VPN 接続ではなく、リモートアクセス VPN 接続を監視する管理者向けに設計されています。

VPN セッションマネージャロールを持つユーザーは、次のことができます。

- Security Cloud Control の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、RA VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。VPN セッションマネージャのユーザーは、自分のトークンを取り消すと、再作成できないことに注意してください。
- インターフェイスからサポートに連絡し、変更ログをエクスポートする。
- 既存の RA VPN セッションを終了する。

VPN セッションマネージャのユーザーは、次のことは**できません**。

- 任意のページで作成、更新、設定、または削除する。
- デバイスをオンボーディングする。
- オブジェクトやポリシーなどの作成に必要なタスクのステップスルーはできるが保存はできない。
- Security Cloud Control ユーザーレコードを作成する。
- ユーザーロールを変更する。
- アクセスルールをポリシーにアタッチまたはデタッチする。

Admin ロール

管理者ユーザーは、Security Cloud Control のあらゆる側面に完全にアクセスできます。管理者ユーザーは次のことができます。

- Security Cloud Control の任意のオブジェクトを作成、読み取り、更新、削除し、設定を行う。
- デバイスをオンボーディングする。

- Security Cloud Control の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。トークンが取り消された場合は、インターフェイスを介してサポートに連絡し、変更ログをエクスポートできます。

管理者ユーザーは次のことを**実行できません**。

- Security Cloud Control ユーザーレコードを作成する。
- ユーザーロールを変更する。

ネットワーク管理者ロール

スーパー管理者ユーザーは、Security Cloud Control のあらゆる側面に完全にアクセスできます。スーパー管理者は次のことができます。

- ユーザーロールを変更する。
- ユーザーレコードを作成する。
- Security Cloud Control の任意のオブジェクトを作成、読み取り、更新、削除し、設定を行う。
- デバイスをオンボーディングする。
- Security Cloud Control の任意のページまたは設定を確認する。
- 任意のページのコンテンツを検索およびフィルタリングする。
- デバイス設定を比較し、変更ログを表示し、VPN マッピングを確認する。
- 任意のページの設定またはオブジェクトに関するすべての警告を表示する。
- 独自の API トークンを生成する、更新する、取り消す。トークンが取り消された場合は、次のことができます。
- インターフェイスからサポートに連絡し、変更ログをエクスポートする。

ユーザーロールのレコードの変更

ユーザーレコードは、現在記録されているユーザーのロールです。テナントに関連付けられているユーザーを調べることにより、各ユーザーがどのロールを使用しているかをレコードによって判断できます。ユーザーロールを変更すると、ユーザーレコードが変更されます。ユーザーのロールは、ユーザー管理テーブルでのロールによって識別されます。詳細については、「ユーザーの管理」を参照してください。

ユーザーレコードを変更するには、ネットワーク管理者である必要があります。テナントにネットワーク管理者がいない場合は、Security Cloud Control サポートまでお問い合わせください。

Security Cloud Control へのユーザーアカウントの追加

Security Cloud Control ユーザーは、認証されて Security Cloud Control テナントにアクセスできるように、Security Cloud Control レコードと対応する IdP アカウントが必要です。この手順では、Cisco Security Cloud Sign On のユーザーアカウントではなく、ユーザーの Security Cloud Control ユーザーレコードを作成します。ユーザーが Cisco Security Cloud Sign On にアカウントを持っていない場合、https://security.cisco.com に移動し、サインイン画面の下部にある **[Sign up]** をクリックして、自己登録できます。

（注） このタスクを実行するには、Security Cloud Control でスーパー管理者のロールが必要です。

ユーザーレコードの作成

次の手順を使用して、適切なユーザーロールを持つユーザーレコードを作成します。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 青いプラスボタン（+）をクリックして、新しいユーザーをテナントに追加します。

ステップ 5 ユーザーの電子メールアドレスを入力します。

（注）
ユーザーの電子メールアドレスは、Cisco Secure Log-On アカウントの電子メールアドレスに対応している必要があります。

ステップ 6 ドロップダウンメニューからユーザーのロールを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

ユーザーロールのユーザーレコードの編集

このタスクを実行するには、ネットワーク管理者のロールが必要です。ログインしている Security Cloud Control ユーザーのロールをネットワーク管理者が変更する場合、そのロールが変更されると、そのユーザーはセッションから自動的にログアウトされます。ユーザーが再度ログインすると、ユーザーは新しいロールを担います。

（注） このタスクを実行するには、Security Cloud Control でスーパー管理者のロールが必要です。

注意 ユーザーレコードのロールを変更すると、ユーザーレコードに関連付けられた API トークンがある場合はそれが削除されます。ユーザーロールが変更されたら、ユーザーは新しい API トークンを生成する必要があります。

ユーザーロールの編集

（注） Security Cloud Control ユーザーがログインしていて、ネットワーク管理者がそのロールを変更した場合、変更を有効にするには、そのユーザーがログアウトして再度ログインする必要があります。

ユーザーレコードで定義されたロールを編集するには、次の手順に従います。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。

ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。

ステップ 4 ユーザーの行にある [編集（Edit）] アイコンをクリックします。

ステップ 5 [ロール（Role）] ドロップダウンメニューからユーザーの新しい [ロール（Role）] を選択します。

ステップ 6 ユーザーレコードに、ユーザーに関連付けられた API トークンがあることが示されている場合は、ユーザーのロールを変更し、結果として API トークンを削除することを確認する必要があります。」

ステップ 7 [v] をクリックします。

ステップ 8 Security Cloud Control が API トークンを削除した場合、ユーザーに連絡し、新しい API トークンを作成できることを知らせます。

（注）
Dynamic Attributes Connector サービスアカウント（csdac-service@tenantname）の API 専用ユーザーの、**[Revoke]**、**[Refresh]**、**[Delete]**、および **[Edit]** オプションが無効になっています。これは、Dynamic Attributes Connector の機能に必要な、この API アカウントの API トークンをお客様が削除、編集、または取り消してしまうのを防ぐためです。

ユーザーロールのユーザーレコードの削除

Security Cloud Control のユーザーレコードを削除すると、ユーザーレコードの Cisco Security Cloud Sign On アカウントとのマッピングが壊れ、関連付けられたユーザーが Security Cloud Control にログインできなくなります。ユーザーレコードを削除すると、そのユーザーレコードに関連付けられている API トークンも削除されます（存在する場合）。Security Cloud Control のユーザーレコードを削除しても、Cisco Security Cloud Sign On のユーザーの IdP アカウントは削除されません。

（注） このタスクを実行するには、Security Cloud Control でスーパー管理者のロールが必要です。

ユーザーレコードの削除

ユーザーレコードに定義されているロールを削除するには、次の手順を実行します。

手順

ステップ 1 Security Cloud Control にログインします。
ステップ 2 Cisco Security Cloud Control ホームページから、**[Products]** > **[Firewall]** を選択します。
ステップ 3 左側のペインで **Administration** > **API User Management** をクリックします。
ステップ 4 削除するユーザーの行のごみ箱アイコン をクリックします。
ステップ 5 [OK] をクリックします。
ステップ 6 [OK] をクリックして、テナントからアカウントを削除することを確認します。

（注）
Dynamic Attributes Connector サービスアカウント（csdac-service@tenantname）の API 専用ユーザーの、**[Revoke]**、**[Refresh]**、**[Delete]**、および **[Edit]** オプションが無効になっています。これは、Dynamic Attributes Connector の機能に必要な、この API アカウントの API トークンをお客様が削除、編集、または取り消してしまうのを防ぐためです。

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。